Broadcom NetXtreme® 57XX User Guide

Information in this document is subject to change without notice.

Broadcom Corporation reserves the right to make changes without further notice to any products or data herein to improve reliability, function, or design. Information furnished by Broadcom Corporation is believed to be accurate and reliable. However, Broadcom Corporation does not assume any liability arising out of the application or use of this information, nor the application or use of any product or circuit described herein, neither does it convey any license under its patent rights or the rights of others.

Last revised: September 2013

INGSRV162-CDUM100-R

Functionality and Features: Broadcom NetXtreme 57XX User Guide

Functional Description

Broadcom NetXtreme Gigabit Ethernet adapters connect a PCI, PCI-X (BCM5701 and BCM5703), or PCI Express™ (BCM5751, BCM5719, BCM5720, BCM5721, and BCM5722) compliant system to a Gigabit Ethernet network. The BCM5714 provides an independent PCI-X bus for peripheral connectivity. Broadcom NetXtreme Gigabit Ethernet adapters incorporate a technology that transfers data at a maximum rate of 1 gigabit per second—10 times the rate of Fast Ethernet adapters.

Broadcom NetXtreme Gigabit Ethernet adapters target the increased congestion experienced at the backbone and system in today's networks and provide a future upgrade path for systems that require more bandwidth than Fast Ethernet can provide.

Using the Broadcom teaming software, you can split your network into virtual LANs (VLANs) as well as group multiple network adapters together into teams to provide network load balancing and fault tolerance functionality. See Teaming and Broadcom Gigabit Ethernet Teaming Services for detailed information about teaming. See Virtual LANs for a description of VLANs. See Configuring Teaming for instructions on configuring teaming and creating VLANs on Windows operating systems.

FEATURES

The following is a list of the Broadcom NetXtreme Gigabit Ethernet adapter features for all supported operating systems:

- Gigabit Ethernet (IEEE Std 802.3-1999)
- Logical Link Control (IEEE Std 802.2)
- Flow Control (IEEE Std 802.3x)
- Standard Ethernet frame size (1518 bytes)
- TBI (SerDes style) transceiver interfaces (except for BCM5721, BCM5751, and BCM5722)
- Jumbo frames (up to 9 KB) (except for BCM5721, BCM5751, and BCM5722)
- Layer-2 Priority Encoding (IEEE 802.1p)
- High-speed on-chip RISC processor
- Adaptive interrupt frequency
- Up to 4 classes of service (CoS)
- Up to 4 send rings and receive rings
- Integrated 96 KB frame buffer memory
- GMI/MII Management Interface
- Statistics for SNMP MIB II, Ethernet-like MIB, and Ethernet MIB (IEEE Std 802.3z, Clause 30)
- 4 unique MAC unicast addresses
- Support for multicast addresses via 128 bits hashing hardware function
- Serial EEPROM or serial NVRAM flash memory
- Supports PXE 2.1 specification (Linux Red Hat PXE Server, Windows Server, Intel APITEST, DOS UNDI)
- JTAG support
- PCI v2.3 32/64-bit, 33/66 MHz Bus Interface (BCM5702)
- PCI-X v1.0 64-bit 100/133 MHz Bus Interface (BCM5703, BCM5704, CIOB-ES)
- PCI Power Management Interface (v1.1)
- PCI Hot-Plug
- ACPI and Wake on LAN support
- 64-bit BAR support
- EM64T processor support
- 3.3 V/1.8 V CMOS with 5V tolerant I/Os
- LiveLink™ (supported in both the 32-bit and 64-bit Windows operating systems
- Self boot

Power Management

Wake on LAN (Magic Packet, Wake Up Frame, specific pattern) is supported at 10/100 Mbps operation only.

NOTES:

- Adapter speed connection when the system is down waiting for a wake-up signal is either 10 Mbps or 100 Mbps, but can return to 1000 Mbps when the system is up and running if connected to a 1000 Mbps capable switch. Systems intending to use Wake on LAN (WOL) should be connected to a switch capable of both 1000 and 10/100 Mbps speeds.
- Broadcom supports Wake on LAN on one adapter in the system at a time.

Adaptive Interrupt Frequency

The adapter driver intelligently adjusts host interrupt frequency based on traffic conditions, to increase overall application throughput. When traffic is light, the adapter driver interrupts the host for each received packet, minimizing latency. When traffic is heavy, the adapter issues one host interrupt for multiple, back-to-back incoming packets, preserving host CPU cycles.

Dual DMA Channels

The PCI interface on Broadcom NetXtreme Gigabit Ethernet adapters contains two independent DMA channels for simultaneous read and write operations.

32-Bit or 64-Bit PCI Bus Master

Compliant with PCI Local Bus Rev 2.3, the PCI interface on Broadcom NetXtreme Gigabit Ethernet adapters is compatible with both 32-bit and 64-bit PCI buses. As a bus master, the adapter requests access to the PCI bus, instead of waiting to be polled.

ASIC with Embedded RISC Processor

The core control for Broadcom NetXtreme Gigabit Ethernet adapters resides in a tightly integrated, high-performance ASIC. The ASIC includes a RISC processor. This functionality provides the flexibility to add new features to the card and adapts it to future network requirements through software downloads. This functionality also enables the adapter drivers to exploit the built-in host offload functions on the adapter as host operating systems are enhanced to take advantage of these functions.

Broadcom Advanced Control Suite

Broadcom Advanced Control Suite (BACS), a component of the Broadcom teaming software, is an integrated utility that provides useful information about each network adapter that is installed in your system. The BACS utility also enables you to perform detailed tests, diagnostics, and analyses on each adapter, as well as to modify property values and view traffic statistics for each adapter. BACS is used on Windows operating systems to configure teaming and to add VLANs. See Using Broadcom Advanced Control Suite for detailed information and instructions.

Supported Operating Environments

The Broadcom NetXtreme Gigabit Ethernet adapter has software support for the following operating systems:

- Microsoft® Windows® (32-bit and 64-bit extended)
- Linux® (32-bit and 64-bit extended)
- VMware
- MS-DOS®
- Sun Solaris
- SCO® UnixWare®
- SCO OpenServer®

Network Link and Activity Indication

For copper-wire Ethernet connections, the state of the network link and activity is indicated by the LEDs on the RJ-45 connector, as described in Table 1: "Network Link and Activity Indicated by RJ-45 Port LEDs," on page 6. Broadcom Advanced Control Suite also provides information about the status of the network link and activity.

Table 1. Network Link and Activity Indicated by RJ-45 Port LEDs

Port LED	*LED Appearance*	*Network State*
Link LED	Off	No link (cable disconnected)
	Continuously illuminated	Link
Activity LED	Off	No network activity
	Blinking	Network activity

Teaming: Broadcom NetXtreme 57XX User Guide

- Overview
- Load Balancing and Fault Tolerance

NOTE: See Broadcom Gigabit Ethernet Teaming Services for detailed information on the following topics:

- Glossary of Terms and Acronyms
- Teaming Concepts
- Software Components
- Hardware Requirements
- Supported Teaming by Processor
- Configuring Teaming by Operating System
- Supported Features by Team Type
- Selecting a Team Type
- Teaming Mechanisms
- Architecture
- Types of Teams
- Driver Support by Operating System
- Supported Teaming Speeds
- Teaming and Other Advanced Networking Features
- General Network Considerations
- Application Considerations
- Troubleshooting Teaming Problems
- Frequently-Asked Questions
- Event Log Messages

Overview

Adapter teaming allows you to group network adapters together to function as a team. The benefits of teaming include allowing membership to VLANs, providing load balancing between adapters, and offering fault tolerance. These benefits can be combined such that you can couple the functionality of load balancing for the load balance members and the capability of employing a failover with having the team participate on different VLANs.

Broadcom Advanced Server Program (BASP) is the Broadcom teaming software for Windows Server 2008 operating systems. For Windows operating systems, BASP is configured through the Broadcom Advanced Control Suite (BACS) utility. For Linux operating systems, teaming is done with channel bonding (see Teaming with Channel Bonding).

BASP supports four types of load balancing teams:

- Smart Load Balancing and Failover
- Link Aggregation (802.3ad)
- Generic Trunking (FEC/GEC)/802.3ad-Draft Static
- SLB (Auto-Fallback Disable)

Load Balancing and Fault Tolerance

Teaming provides traffic load balancing and fault tolerance (redundant adapter operation in the event that a network connection fails). When multiple adapters are installed in the same system, they can be grouped with up to four teams.

Each team can consist of up to eight adapters, with one adapter used as a standby for Smart Load Balancing and Failover (SLB) or SLB (Auto-Fallback Disabled) team types. If traffic is not identified on any of the adapter team member connections due to failure of the adapter, cable, or switch, the load will be distributed to the remaining team members with an active connection. In the event that all primary adapters fail, traffic will be distributed to the standby adapter. Existing sessions are maintained with no impact on the user.

Types of Teams

The available types of teams for the supported operating systems are shown in the following table:

Table 1. Types of Teams

Operating System	Available Types of Teams
Windows Server 2008 and Windows Server 2012	Smart Load Balancing and Failover Link Aggregation (802.3ad) Generic Trunking (FEC/GEC)/802.3ad-Draft Static SLB (Auto-Fallback Disable) **NOTE**: Windows Server 2012 provides built-in teaming support, called NIC Teaming. It is not recommended that users enable teams through NIC Teaming and BASP at the same time on the same adapters.
Linux	Team adapters using the bonding kernel module and a channel bonding interface. See your Red Hat documentation for more information.

Smart Load Balancing™ and Failover

Smart Load Balancing™ and Failover is the Broadcom implementation of load balancing based on IP flow. This feature supports balancing IP traffic across multiple adapters (team members) in a bidirectional manner. In this type of team, all adapters in the team have separate MAC addresses. This type of team provides automatic fault detection and dynamic failover to other team member or to a hot standby member. This is done independently of Layer 3 protocol (IP, IPX, NetBEUI); rather, it works with existing Layer 2 and Layer 3 switches. No switch configuration (such as trunk, link aggregation) is necessary for this type of team to work.

NOTES:

- If you do not enable LiveLink™ when configuring SLB teams, disabling Spanning Tree Protocol (STP) at the switch or port is recommended. This minimizes the downtime due to spanning tree loop determination when failing over. LiveLink mitigates such issues.
- IPX balances only on the transmit side of the team; other protocols are limited to the primary adapter.
- If a team member is linked at 1000 Mbit/s and another team member is linked at 100 Mbit/s, most of the traffic is handled by the 1000 Mbit/s team member.

Link Aggregation (802.3ad)

This mode supports link aggregation and conforms to the IEEE 802.3ad (LACP) specification. Configuration software allows you to dynamically configure which adapters you want to participate in a given team. If the link partner is not correctly configured for 802.3ad link configuration, errors are detected and noted. With this mode, all adapters in the team are configured to receive packets for the same MAC address. The outbound load-balancing scheme is determined by our BASP driver. The team link partner determines the load-balancing scheme for inbound packets. In this mode, at least one of the link partners must be in active mode.

Generic Trunking (FEC/GEC)/802.3ad-Draft Static

The Generic Trunking (FEC/GEC)/802.3ad-Draft Static type of team is very similar to the Link Aggregation (802.3ad) type of team in that all adapters in the team are configured to receive packets for the same MAC address. The Generic Trunking (FEC/GEC)/802.3ad-Draft Static) type of team, however, does not provide LACP or marker protocol support. This type of team supports a variety of environments in which the adapter link partners are statically configured to support a proprietary trunking mechanism. For instance, this type of team could be used to support Lucent's OpenTrunk or Cisco's Fast EtherChannel (FEC). Basically, this type of team is a light version of the Link Aggregation (802.3ad) type of team. This approach is much simpler, in that there is not a formalized link aggregation control protocol (LACP). As with the other types of teams, the creation of teams and the allocation of physical adapters to various teams is done statically through user configuration software.

The Generic Trunking (FEC/GEC/802.3ad-Draft Static) type of team supports load balancing and failover for both outbound and inbound traffic.

SLB (Auto-Fallback Disable)

The SLB (Auto-Fallback Disable) type of team is identical to the Smart Load Balancing and Failover type of team, with the following exception—when the standby member is active, if a primary member comes back on line, the team continues using the standby member, rather than switching back to the primary member.

If any primary adapter assigned to a team is disabled, the team functions as a Smart Load Balancing and Failover type of team in which auto-fallback occurs.

All primary interfaces in a team participate in load-balancing operations by sending and receiving a portion of the total traffic. Standby interfaces take over in the event that all primary interfaces have lost their links.

Failover teaming provides redundant adapter operation (fault tolerance) in the event that a network connection fails. If the primary adapter in a team is disconnected because of failure of the adapter, cable, or switch port, the secondary team member becomes active, redirecting both inbound and outbound traffic originally assigned to the primary adapter. Sessions will be maintained, causing no impact to the user.

Limitations of Smart Load Balancing and Failover/SLB (Auto-Fallback Disable) Types of Teams

Smart Load Balancing™ (SLB) is a protocol-specific scheme. The level of support for IP, IPX, and NetBEUI protocols is listed below.

Table 2. Smart Load Balancing

Operating System	**Failover/Fallback—All Broadcom**			**Failover/Fallback—Multivendor**		
Protocol	**IP**	**IPX**	**NetBEUI**	**IP**	**IPX**	**NetBEUI**
Windows Server 2008	Y	Y	N/S	Y	N	N/S
Red Hat Linux 3 and 4	Y	N/S	N/S	Y	N/S	N/S
Operating System	**Load Balance—All Broadcom**			**Load Balance—Multivendor**		
Protocol	**IP**	**IPX**	**NetBEUI**	**IP**	**IPX**	**NetBEUI**
Windows Server 2008	Y	Y	N/S	Y	N	N/S
Red Hat Linux 3 and 4	Y	N/S	N/S	Y	N/S	N/S

Legend:	Y = yes
	N = no
	N/S = not supported

The Smart Load Balancing type of team works with all Ethernet switches without having to configure the switch ports to any special trunking mode. Only IP traffic is load-balanced in both inbound and outbound directions. IPX traffic is load-balanced in the outbound direction only. Other protocol packets are sent and received through one primary interface only. Failover for non-IP traffic is supported only for Broadcom network adapters. The Generic Trunking type of team requires the Ethernet switch to support some form of port trunking mode (for example, Cisco's Gigabit EtherChannel or other switch vendor's Link Aggregation mode). The Generic Trunking type of team is protocol-independent, and all traffic should be load-balanced and fault-tolerant.

NOTE: If you do not enable LiveLink™ when configuring teams, disabling Spanning Tree Protocol (STP) at the switch is recommended. This minimizes the downtime due to the spanning tree loop determination when failing over. LiveLink mitigates such issues.

LiveLink™ Functionality

LiveLink™ functionality is a feature of BASP that is available only for the Smart Load Balancing™ and Failover type of teaming. The purpose of LiveLink is to detect network connectivity beyond the switch and to route traffic only through team members that have a live link. This function is accomplished though the teaming software (see Configuring LiveLink for a Smart Load Balancing and Failover and SLB (Auto-Fallback Disable) Team). The teaming software periodically probes (issues a link packet from each team member) one or more specified target network adapter(s). The probe target(s) responds when it receives the link packet. If a team member does not detect a response within a specified amount of time after a specified number of retries, the teaming software discontinues passing traffic through that team member. Later, if that team member begins to detect a response from a probe target, this indicates that the link has been restored, and the teaming software automatically resumes passing traffic through that team member. LiveLink works only with TCP/IP.

LiveLink™ functionality is supported in both 32-bit and 64-bit Windows operating systems. For similar functionality in Linux operating systems, refer to Channel Bonding in your Red Hat documentation.

Teaming and Large Send Offload/Checksum Offload Support

Large Send Offload (LSO) and Checksum Offload are enabled for a team only when all of the members support and are configured for the feature.

Broadcom Gigabit Ethernet Teaming Services: Broadcom NetXtreme 57XX User Guide

INTRODUCTION

This section describes the technology and implementation considerations when working with the network teaming services offered by the Broadcom software shipped with systems. The goal of Broadcom teaming services is to provide fault tolerance and link aggregation across a team of two or more adapters. The information in this document is provided to assist IT professionals during the deployment and troubleshooting of system applications that require network fault tolerance and load balancing.

GLOSSARY

Table 1. Glossary

Item	Definition
ARP	Address Resolution Protocol
BACS	Broadcom Advanced Control Suite
BASP	Broadcom Advanced Server Program (intermediate driver)
DNS	domain name service
G-ARP	Gratuitous Address Resolution Protocol
Generic Trunking (FEC/GEC)/ 802.3ad-Draft Static	Switch-dependent load balancing and failover type of team in which the intermediate driver manages outgoing traffic and the switch manages incoming traffic.
HSRP	Hot Standby Router Protocol
ICMP	Internet Control Message Protocol
IGMP	Internet Group Management Protocol
IP	Internet Protocol
LACP	Link Aggregation Control Protocol
Link Aggregation (802.3ad)	Switch-dependent load balancing and failover type of team with LACP in which the intermediate driver manages outgoing traffic and the switch manages incoming traffic.
LOM	LAN on Motherboard
MAC	media access control
NDIS	Network Driver Interface Specification
NLB	Network Load Balancing (Microsoft)
PXE	Preboot Execution Environment
RAID	Redundant array of inexpensive disks
Smart Load Balance and Failover	Switch-independent failover type of team in which the primary team member handles all incoming and outgoing traffic while the standby team member is idle until a failover event (for example, loss of link occurs). The intermediate driver (BASP) manages incoming/outgoing traffic.
Smart Load Balancing (SLB)	Switch-independent load balancing and failover type of team, in which the intermediate driver manages outgoing/incoming traffic.
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
WINS	Windows name service
WLBS	Windows Load Balancing Service

TEAMING CONCEPTS

- Network Addressing
- Teaming and Network Addresses
- Description of Teaming Types

The concept of grouping multiple physical devices to provide fault tolerance and load balancing is not new. It has been around for years. Storage devices use RAID technology to group individual hard drives. Switch ports can be grouped together using technologies such as Cisco Gigabit EtherChannel, IEEE 802.3ad Link Aggregation, Bay Network Multilink Trunking, and Extreme Network Load Sharing. Network interfaces on systems can be grouped together into a team of physical ports called a virtual adapter.

Network Addressing

To understand how teaming works, it is important to understand how node communications work in an Ethernet network. This document is based on the assumption that the reader is familiar with the basics of IP and Ethernet network communications. The following information provides a high-level overview of the concepts of network addressing used in an Ethernet network.

Every Ethernet network interface in a host platform, such as a computer system, requires a globally unique Layer 2 address and at least one globally unique Layer 3 address. Layer 2 is the Data Link Layer, and Layer 3 is the Network layer as defined in the OSI model. The Layer 2 address is assigned to the hardware and is often referred to as the MAC address or physical address. This address is pre-programmed at the factory and stored in NVRAM on a network interface card or on the system motherboard for an embedded LAN interface. The Layer 3 addresses are referred to as the protocol or logical address assigned to the software stack. IP and IPX are examples of Layer 3 protocols. In addition, Layer 4 (Transport Layer) uses port numbers for each network upper level protocol such as Telnet or FTP. These port numbers are used to differentiate traffic flows across applications. Layer 4 protocols such as TCP or UDP are most commonly used in today’s networks. The combination of the IP address and the TCP port number is called a socket.

Ethernet devices communicate with other Ethernet devices using the MAC address, not the IP address. However, most applications work with a host name that is translated to an IP address by a Naming Service such as WINS and DNS. Therefore, a method of identifying the MAC address assigned to the IP address is required. The Address Resolution Protocol for an IP network provides this mechanism. For IPX, the MAC address is part of the network address and ARP is not required. ARP is implemented using an ARP Request and ARP Reply frame. ARP Requests are typically sent to a broadcast address while the ARP Reply is typically sent as unicast traffic. A unicast address corresponds to a single MAC address or a single IP address. A broadcast address is sent to all devices on a network.

Teaming and Network Addresses

A team of adapters function as a single virtual network interface and does not appear any different to other network devices than a non-teamed adapter. A virtual network adapter advertises a single Layer 2 and one or more Layer 3 addresses. When the teaming driver initializes, it selects one MAC address from one of the physical adapters that make up the team to be the Team MAC address. This address is typically taken from the first adapter that gets initialized by the driver. When the system hosting the team receives an ARP request, it selects one MAC address from among the physical adapters in the team to use as the source MAC address in the ARP Reply. In Windows operating systems, the IPCONFIG /all command shows the IP and MAC address of the virtual adapter and not the individual physical adapters. The protocol IP address is assigned to the virtual network interface and not to the individual physical adapters.

For switch-independent teaming modes, all physical adapters that make up a virtual adapter must use the unique MAC address assigned to them when transmitting data. That is, the frames that are sent by each of the physical adapters in the team must use a unique MAC address to be IEEE compliant. It is important to note that ARP cache entries are not learned from received frames, but only from ARP requests and ARP replies.

Description of Teaming Types

- Smart Load Balancing and Failover
- Generic Trunking
- Link Aggregation (IEEE 802.3ad LACP)
- SLB (Auto-Fallback Disable)

There are three methods for classifying the supported teaming types:

- One is based on whether the switch port configuration must also match the adapter teaming type.
- The second is based on the functionality of the team, whether it supports load balancing and failover or just failover.
- The third is based on whether the Link Aggregation Control Protocol is used or not.

Table 2 shows a summary of the teaming types and their classification.

Table 2. Available Teaming Types

Teaming Type	Switch-Dependent (Switch must support specific type of team)	Link Aggregation Control Protocol support is required on the switch	Load Balancing	Failover
Smart Load Balancing and Failover (with two to eight load balance team members)			●	●
SLB (Auto-Fallback Disable)				●
Link Aggregation (802.3ad)	●	●	●	●
Generic Trunking (FEC/GEC)/802.3ad-Draft Static	●		●	●

Smart Load Balancing and Failover

The Smart Load Balancing™ and Failover type of team provides both load balancing and failover when configured for load balancing, and only failover when configured for fault tolerance. This type of team works with any Ethernet switch and requires no trunking configuration on the switch. The team advertises multiple MAC addresses and one or more IP addresses (when using secondary IP addresses). The team MAC address is selected from the list of load balance members. When the system receives an ARP request, the software-networking stack will always send an ARP Reply with the team MAC address. To begin the load balancing process, the teaming driver will modify this ARP Reply by changing the source MAC address to match one of the physical adapters.

Smart Load Balancing enables both transmit and receive load balancing based on the Layer 3/Layer 4 IP address and TCP/UDP port number. In other words, the load balancing is not done at a byte or frame level but on a TCP/UDP session basis. This methodology is required to maintain in-order delivery of frames that belong to the same socket conversation. Load balancing is supported on 2 to 8 ports. These ports can include any combination of add-in adapters and LAN on Motherboard (LOM) devices. Transmit load balancing is achieved by creating a hashing table using the source and destination IP addresses and TCP/UDP port numbers.The same combination of source and destination IP addresses and TCP/UDP port numbers will generally yield the same hash index and therefore point to the same port in the team. When a port is selected to carry all the frames of a given socket, the unique MAC address of the physical adapter is included in the frame, and not the team MAC address. This is required to comply with the IEEE 802.3 standard. If two adapters transmit using the same MAC address, then a duplicate MAC address situation would occur that the switch could not handle.

Receive load balancing is achieved through an intermediate driver by sending gratuitous ARPs on a client-by-client basis using the unicast address of each client as the destination address of the ARP request (also known as a directed ARP). This is considered client load balancing and not traffic load balancing. When the intermediate driver detects a significant load imbalance between the physical adapters in an SLB team, it will generate G-ARPs in an effort to redistribute incoming frames. The intermediate driver (BASP) does not answer ARP requests; only the software protocol stack provides the required ARP Reply. It is important to understand that receive load balancing is a function of the number of clients that are connecting to the system through the team interface.

SLB receive load balancing attempts to load balance incoming traffic for client machines across physical ports in the team. It uses a modified gratuitous ARP to advertise a different MAC address for the team IP Address in the sender physical and protocol address. This G-ARP is unicast with the MAC and IP Address of a client machine in the target physical and protocol address respectively. This causes the target client to update its ARP cache with a new MAC address map to the team IP address. G-ARPs are not broadcast because this would cause all clients to send their traffic to the same port. As a result, the benefits achieved through client load balancing would be eliminated, and could cause out-of-order frame delivery. This receive load balancing scheme works as long as all clients and the teamed system are on the same subnet or broadcast domain.

When the clients and the system are on different subnets, and incoming traffic has to traverse a router, the received traffic destined for the system is not load balanced. The physical adapter that the intermediate driver has selected to carry the IP flow carries all of the traffic. When the router sends a frame to the team IP address, it broadcasts an ARP request (if not in the ARP cache). The server software stack generates an ARP reply with the team MAC address, but the intermediate driver modifies the ARP reply and sends it over a particular physical adapter, establishing the flow for that session.

The reason is that ARP is not a routable protocol. It does not have an IP header and therefore, is not sent to the router or default gateway. ARP is only a local subnet protocol. In addition, since the G-ARP is not a broadcast packet, the router will not process it and will not update its own ARP cache.

The only way that the router would process an ARP that is intended for another network device is if it has Proxy ARP enabled and the host has no default gateway. This is very rare and not recommended for most applications.

Transmit traffic through a router will be load balanced as transmit load balancing is based on the source and destination IP address and TCP/UDP port number. Since routers do not alter the source and destination IP address, the load balancing algorithm works as intended.

Configuring routers for Hot Standby Routing Protocol (HSRP) does not allow for receive load balancing to occur in the adapter team. In general, HSRP allows for two routers to act as one router, advertising a virtual IP and virtual MAC address. One physical router is the active interface while the other is standby. Although HSRP can also load share nodes (using different default gateways on the host nodes) across multiple routers in HSRP groups, it always points to the primary MAC address of the team.

Generic Trunking

Generic Trunking is a switch-assisted teaming mode and requires configuring ports at both ends of the link: server interfaces and switch ports. This is often referred to as Cisco Fast EtherChannel or Gigabit EtherChannel. In addition, generic trunking supports similar implementations by other switch OEMs such as Extreme Networks Load Sharing and Bay Networks or IEEE 802.3ad Link Aggregation static mode. In this mode, the team advertises one MAC Address and one IP Address when the protocol stack responds to ARP Requests. In addition, each physical adapter in the team uses the same team MAC address when transmitting frames. This is possible since the switch at the other end of the link is aware of the teaming mode and will handle the use of a single MAC address by every port in the team. The forwarding table in the switch will reflect the trunk as a single virtual port.

In this teaming mode, the intermediate driver controls load balancing and failover for outgoing traffic only, while incoming traffic is controlled by the switch firmware and hardware. As is the case for Smart Load Balancing, the BASP intermediate driver uses the IP/TCP/UDP source and destination addresses to load balance the transmit traffic from the server. Most switches implement an XOR hashing of the source and destination MAC address.

Link Aggregation (IEEE 802.3ad LACP)

Link Aggregation is similar to Generic Trunking except that it uses the Link Aggregation Control Protocol to negotiate the ports that will make up the team. LACP must be enabled at both ends of the link for the team to be operational. If LACP is not available at both ends of the link, 802.3ad provides a manual aggregation that only requires both ends of the link to be in a link up state. Because manual aggregation provides for the activation of a member link without performing the LACP message exchanges, it should not be considered as reliable and robust as an LACP negotiated link. LACP automatically determines which member links can be aggregated and then aggregates them. It provides for the controlled addition and removal of physical links for the link aggregation so that no frames are lost or duplicated. The removal of aggregate link members is provided by the marker protocol that can be optionally enabled for Link Aggregation Control Protocol (LACP) enabled aggregate links.

The Link Aggregation group advertises a single MAC address for all the ports in the trunk. The MAC address of the Aggregator can be the MAC addresses of one of the MACs that make up the group. LACP and marker protocols use a multicast destination address.

The Link Aggregation control function determines which links may be aggregated and then binds the ports to an Aggregator function in the system and monitors conditions to determine if a change in the aggregation group is required. Link aggregation combines the individual capacity of multiple links to form a high performance virtual link. The failure or replacement of a link in an LACP trunk will not cause loss of connectivity. The traffic will simply be failed over to the remaining links in the trunk.

SLB (Auto-Fallback Disable)

This type of team is identical to the Smart Load Balance and Failover type of team, with the following exception—when the standby member is active, if a primary member comes back on line, the team continues using the standby member rather than switching back to the primary member. This type of team is supported only for situations in which the network cable is disconnected and reconnected to the network adapter. It is not supported for situations in which the adapter is removed/ installed through Device Manager or Hot-Plug PCI.

If any primary adapter assigned to a team is disabled, the team functions as a Smart Load Balancing and Failover type of team in which auto-fallback occurs.

SOFTWARE COMPONENTS

Teaming is implemented via an NDIS intermediate driver in the Windows Operating System environment. This software component works with the miniport driver, the NDIS layer, and the protocol stack to enable the teaming architecture (see Figure 1). The miniport driver controls the host LAN controller directly to enable functions such as sends, receives, and interrupt processing. The intermediate driver fits between the miniport driver and the protocol layer multiplexing several miniport driver instances, and creating a virtual adapter that looks like a single adapter to the NDIS layer. NDIS provides a set of library functions to enable the communications between either miniport drivers or intermediate drivers and the protocol stack. The protocol stack implements IP, IPX and ARP. A protocol address such as an IP address is assigned to each miniport device instance, but when an Intermediate driver is installed, the protocol address is assigned to the virtual team adapter and not to the individual miniport devices that make up the team.

The Broadcom supplied teaming support is provided by three individual software components that work together and are supported as a package. When one component is upgraded, all the other components must be upgraded to the supported versions. Table 3 describes the three software components and their associated files for supported operating systems.

Table 3. Broadcom Teaming Software Component

Software Component	Broadcom Name	Windows	Linux
Miniport Driver	Broadcom Base Driver	B57xp32.sys B57w2k.sys B57amd64.sys B57xp64.sys	tg3
Intermediate Driver	Broadcom Advanced Server Program (BASP)	Baspxp32.sys Baspw2k.sys Basamd64.sys Baspxp64.sys	bonding
Configuration User Interface	Broadcom Advanced Control Suite (BACS)	BACS	N/A

Hardware Requirements

- Repeater Hub
- Switching Hub
- Router

The various teaming modes described in this document place certain restrictions on the networking equipment used to connect clients to teamed systems. Each type of network interconnect technology has an effect on teaming as described in the following sections.

Repeater Hub

A Repeater Hub allows a network administrator to extend an Ethernet network beyond the limits of an individual segment. The repeater regenerates the input signal received on one port onto all other connected ports, forming a single collision domain. This means that when a station attached to a repeater sends an Ethernet frame to another station, every station within the same collision domain will also receive that message. If two stations begin transmitting at the same time, a collision occurs, and each transmitting station must retransmit its data after waiting a random amount of time.

The use of a repeater requires that each station participating within the collision domain operate in half-duplex mode. Although half-duplex mode is supported for Gigabit Ethernet adapters in the IEEE 802.3 specification, half-duplex mode is not supported by the majority of Gigabit Ethernet adapter manufacturers. Therefore, half-duplex mode is not considered here.

Teaming across hubs is supported for troubleshooting purposes (such as connecting a network analyzer) for SLB teams only.

Switching Hub

Unlike a repeater hub, a switching hub (or more simply a switch) allows an Ethernet network to be broken into multiple collision domains. The switch is responsible for forwarding Ethernet packets between hosts based solely on Ethernet MAC addresses. A physical network adapter that is attached to a switch may operate in half-duplex or full-duplex mode.

To support Generic Trunking and 802.3ad Link Aggregation, a switch must specifically support such functionality. If the switch does not support these protocols, it may still be used for Smart Load Balancing.

Router

A router is designed to route network traffic based on Layer 3 or higher protocols, although it often also works as a Layer 2 device with switching capabilities. The teaming of ports connected directly to a router is not supported.

Supported Teaming by Processor

All team types are supported by the IA-32, IA-64, AMD-64, and EM64T processors.

Configuring Teaming by Operating System

Table 4 lists the tools used to configure teaming in the supported operating system environments.

Table 4. Configuration Tools

Operating System	Configuration Tool
Windows Server 2008, 2012	BACS utility
Linux	Bonding

The Broadcom Advanced Control Suite (BACS) utility is designed to run in 32-bit and 64-bit Windows Server 2008. BACS is used to configure load balancing and fault tolerance teaming, and VLANs. In addition, it displays the MAC address, driver version, and status information about each network adapter. BACS also includes a number of diagnostics tools such as hardware diagnostics, cable testing, and a network topology test.

Supported Features by Team Type

Table 5 provides a feature comparison across the team types. Use this table to determine the best type of team for your application. The teaming software supports up to eight ports in a single team and up to four teams in a single system. The four teams can be any combination of the supported teaming types, but each team must be on a separate network or subnet.

Table 5. Comparison of Team Types

Type of Team	Fault Tolerance	Load Balancing	Switch-Dependent Static Trunking	Switch-Independent Dynamic Link Aggregation (IEEE 802.3ad)
Function	SLB with Standby[a]	SLB	Generic Trunking	Link Aggregation
Number of ports per team (same broadcast domain)	2–8	2–8	2–8	2–8
Number of teams	4	4	4	4
Adapter fault tolerance	Yes	Yes	Yes	Yes
Switch link fault tolerance (same broadcast domain)	Yes	Yes	Switch-dependent	Switch-dependent
TX load balancing	No	Yes	Yes	Yes
RX load balancing	No	Yes	Yes (performed by the switch)	Yes (performed by the switch)
Requires compatible switch	No	No	Yes	Yes
Heartbeats to check connectivity	No	No	No	No
Mixed media (adapters with different media)	Yes	Yes	Yes (switch-dependent)	Yes
Mixed speeds (adapters that do not support a common speed(s), but can operate at different speeds)	Yes	Yes	No	No
Mixed speeds (adapters that support a common speed(s), but can operate at different speeds)	Yes	Yes	No (must be the same speed)	Yes

Table 5. Comparison of Team Types (Cont.)

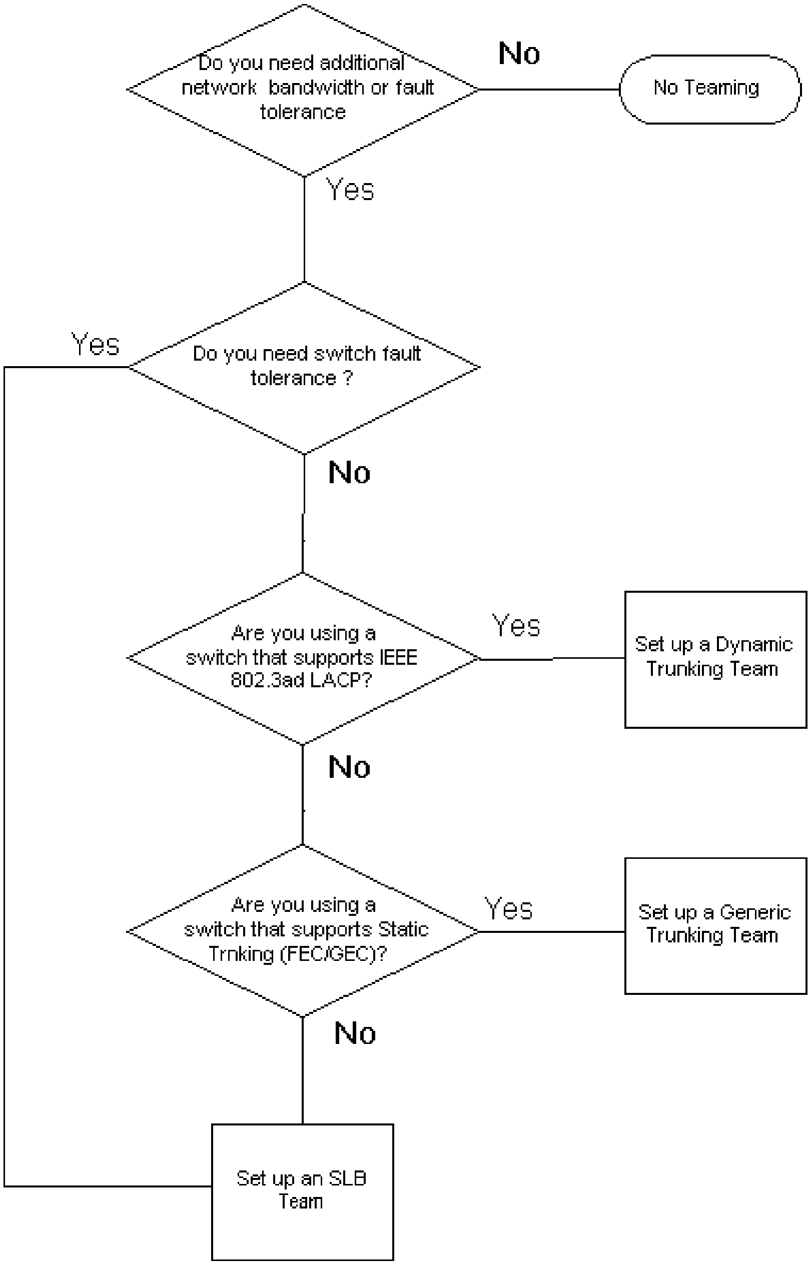
Type of Team	Fault Tolerance	Load Balancing	Switch-Dependent Static Trunking	Switch-Independent Dynamic Link Aggregation (IEEE 802.3ad)
Load balances TCP/IP	No	Yes	Yes	Yes
Mixed vendor teaming	Yes[b]	Yes[b]	Yes[b]	Yes[b]
Load balances non-IP	No	Yes (IPX outbound traffic only)	Yes	Yes
Same MAC address for all team members	No	No	Yes	Yes
Same IP address for all team members	Yes	Yes	Yes	Yes
Load balancing by IP address	No	Yes	Yes	Yes
Load balancing by MAC address	No	Yes (used for no-IP/IPX)	Yes	Yes

[a] SLB with one primary and one standby member.
[b] Requires at least one Broadcom adapter in the team.

SELECTING A TEAM TYPE

The following flow chart provides the decision flow when planning for teaming. The primary rationale for teaming is the need for additional network bandwidth and fault tolerance. Teaming offers link aggregation and fault tolerance to meet both of these requirements. Preference teaming should be selected in the following order: Link Aggregation as the first choice, Generic Trunking as the second choice, and SLB teaming as the third choice when using unmanaged switches or switches that do not support the first two options. If switch fault tolerance is a requirement, then SLB is the only choice (see Figure 1).

Figure 1. Process for Selecting a Team Type

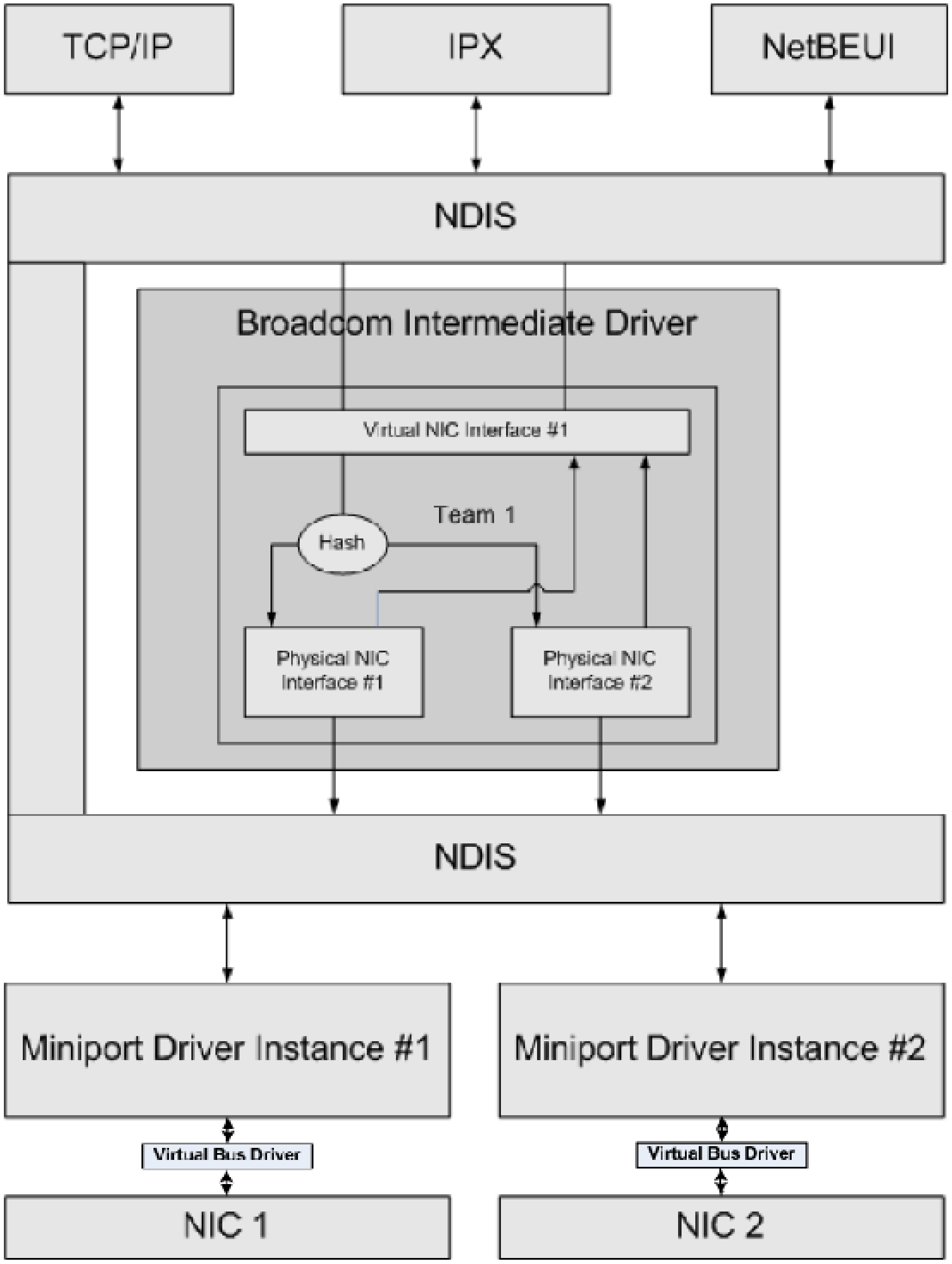

Do you need additional network bandwidth or fault tolerance
No
No Teaming
Yes
Yes
Do you need switch fault tolerance ?
No
Are you using a switch that supports IEEE 802.3ad LACP?
Yes
Set up a Dynamic Trunking Team
No
Are you using a switch that supports Static Trnking (FEC/GEC)?
Yes
Set up a Generic Trunking Team
No
Set up an SLB Team

TEAMING MECHANISMS

ARCHITECTURE

The Broadcom Advanced Server Program is implemented as an NDIS intermediate driver (see Figure 2). It operates below protocol stacks such as TCP/IP and IPX and appears as a virtual adapter. This virtual adapter inherits the MAC Address of the first port initialized in the team. A Layer 3 address must also be configured for the virtual adapter. The primary function of BASP is to balance inbound (for SLB) and outbound traffic (for all teaming modes) among the physical adapters installed on the system selected for teaming. The inbound and outbound algorithms are independent and orthogonal to each other. The outbound traffic for a particular session can be assigned to a given port while its corresponding inbound traffic can be assigned to a different port.

Figure 2. Intermediate Driver


TCP/IP
IPX
NetBEUI
NDIS
Broadcom Intermediate Driver
Virtual NIC Interface #1
Team 1
Hash
Physical NIC Interface #1
Physical NIC Interface #2
NDIS
Miniport Driver Instance #1
Miniport Driver Instance #2
Virtual Bus Driver
Virtual Bus Driver
NIC 1
NIC 2

Outbound Traffic Flow

The Broadcom Intermediate Driver manages the outbound traffic flow for all teaming modes. For outbound traffic, every packet is first classified into a flow, and then distributed to the selected physical adapter for transmission. The flow classification involves an efficient hash computation over known protocol fields. The resulting hash value is used to index into an Outbound Flow Hash Table.The selected Outbound Flow Hash Entry contains the index of the selected physical adapter responsible for transmitting this flow. The source MAC address of the packets will then be modified to the MAC address of the selected physical adapter. The modified packet is then passed to the selected physical adapter for transmission.

The outbound TCP and UDP packets are classified using Layer 3 and Layer 4 header information. This scheme improves the load distributions for popular Internet protocol services using well-known ports such as HTTP and FTP. Therefore, BASP performs load balancing on a TCP session basis and not on a packet-by-packet basis.

In the Outbound Flow Hash Entries, statistics counters are also updated after classification. The load-balancing engine uses these counters to periodically distribute the flows across teamed ports. The outbound code path has been designed to achieve best possible concurrency where multiple concurrent accesses to the Outbound Flow Hash Table are allowed.

For protocols other than TCP/IP, the first physical adapter will always be selected for outbound packets. The exception is Address Resolution Protocol (ARP), which is handled differently to achieve inbound load balancing.

Inbound Traffic Flow (SLB Only)

The Broadcom intermediate driver manages the inbound traffic flow for the SLB teaming mode. Unlike outbound load balancing, inbound load balancing can only be applied to IP addresses that are located in the same subnet as the load-balancing server. Inbound load balancing exploits a unique characteristic of Address Resolution Protocol (RFC0826), in which each IP host uses its own ARP cache to encapsulate the IP Datagram into an Ethernet frame. BASP carefully manipulates the ARP response to direct each IP host to send the inbound IP packet to the desired physical adapter. Therefore, inbound load balancing is a plan-ahead scheme based on statistical history of the inbound flows. New connections from a client to the server will always occur over the primary physical adapter (because the ARP Reply generated by the operating system protocol stack will always associate the logical IP address with the MAC address of the primary physical adapter).

Like the outbound case, there is an Inbound Flow Head Hash Table. Each entry inside this table has a singly linked list and each link (Inbound Flow Entries) represents an IP host located in the same subnet.

When an inbound IP Datagram arrives, the appropriate Inbound Flow Head Entry is located by hashing the source IP address of the IP Datagram. Two statistics counters stored in the selected entry are also updated. These counters are used in the same fashion as the outbound counters by the load-balancing engine periodically to reassign the flows to the physical adapter.

On the inbound code path, the Inbound Flow Head Hash Table is also designed to allow concurrent access. The link lists of Inbound Flow Entries are only referenced in the event of processing ARP packets and the periodic load balancing. There is no per packet reference to the Inbound Flow Entries. Even though the link lists are not bounded; the overhead in processing each non-ARP packet is always a constant. The processing of ARP packets, both inbound and outbound, however, depends on the number of links inside the corresponding link list.

On the inbound processing path, filtering is also employed to prevent broadcast packets from looping back through the system from other physical adapters.

Protocol Support

ARP and IP/TCP/UDP flows are load balanced. If the packet is an IP protocol only, such as ICMP or IGMP, then all data flowing to a particular IP address will go out through the same physical adapter. If the packet uses TCP or UDP for the L4 protocol, then the port number is added to the hashing algorithm, so two separate L4 flows can go out through two separate physical adapters to the same IP address.

For example, assume the client has an IP address of 10.0.0.1. All IGMP and ICMP traffic will go out the same physical adapter because only the IP address is used for the hash. The flow would look something like this:

IGMP ------> PhysAdapter1 ------> 10.0.0.1

ICMP ------> PhysAdapter1 ------> 10.0.0.1

If the server also sends an TCP and UDP flow to the same 10.0.0.1 address, they can be on the same physical adapter as IGMP and ICMP, or on completely different physical adapters from ICMP and IGMP. The stream may look like this:

IGMP ------> PhysAdapter1 ------> 10.0.0.1

ICMP ------> PhysAdapter1 ------> 10.0.0.1

TCP------> PhysAdapter1 ------> 10.0.0.1

UDP------> PhysAdatper1 ------> 10.0.0.1

Or the streams may look like this:

IGMP ------> PhysAdapter1 ------> 10.0.0.1

ICMP ------> PhysAdapter1 ------> 10.0.0.1

TCP------> PhysAdapter2 ------> 10.0.0.1

UDP------> PhysAdatper3 ------> 10.0.0.1

The actual assignment between adapters may change over time, but any protocol that is not TCP/UDP based goes over the same physical adapter because only the IP address is used in the hash.

Performance

Modern network interface cards provide many hardware features that reduce CPU utilization by offloading certain CPU intensive operations (see Teaming and Other Advanced Networking Properties). In contrast, the BASP intermediate driver is a purely software function that must examine every packet received from the protocol stacks and react to its contents before sending it out through a particular physical interface. Though the BASP driver can process each outgoing packet in near constant time, some applications that may already be CPU bound may suffer if operated over a teamed interface. Such an application may be better suited to take advantage of the failover capabilities of the intermediate driver rather than the load balancing features, or it may operate more efficiently over a single physical adapter that provides a particular hardware feature such as Large Send Offload.

Types of Teams

Switch-Independent

The Broadcom Smart Load Balancing type of team allows two to eight physical adapters to operate as a single virtual adapter. The greatest benefit of the SLB type of team is that it operates on any IEEE compliant switch and requires no special configuration.

Smart Load Balancing and Failover

SLB provides for switch-independent, bidirectional, fault-tolerant teaming and load balancing. Switch independence implies that there is no specific support for this function required in the switch, allowing SLB to be compatible with all switches. Under SLB, all adapters in the team have separate MAC addresses. The load-balancing algorithm operates on Layer 3 addresses of the source and destination nodes, which enables SLB to load balance both incoming and outgoing traffic.

The BASP intermediate driver continually monitors the physical ports in a team for link loss. In the event of link loss on any port, traffic is automatically diverted to other ports in the team. The SLB teaming mode supports switch fault tolerance by allowing teaming across different switches- provided the switches are on the same physical network or broadcast domain.

Network Communications

The following are the key attributes of SLB:

- **Failover mechanism** (link loss detection)
- **Load balancing algorithm.** Inbound and outbound traffic are balanced through a Broadcom proprietary mechanism based on L4 flows.
- **Outbound load balancing using MAC address is not supported.**
- **Outbound load balancing using IP address is supported.**
- **Multivendor teaming is supported** (must include at least 1 Broadcom Ethernet adapter as a team member).

Applications

The Smart Load Balance and Failover algorithm is most appropriate in home and small business environments where cost is a concern or commodity switching equipment is used. Smart Load Balance and Failover teaming works with unmanaged Layer 2 switches and is a cost-effective way of getting redundancy and link aggregation at the system. Smart Load Balance and Failover also supports the teaming physical adapters having different link capabilities. In addition, Smart Load Balance and Failover is recommended when switch fault tolerance is required.

Configuration Recommendations

The Smart Load Balance and Failover type of team supports connecting the teamed ports to hubs and switches if they are on the same broadcast domain. It does not support connecting to a router or Layer 3 switches because the ports must be on the same subnet.

Switch-Dependent

Generic Static Trunking

This mode supports a variety of environments where the adapter link partners are statically configured to support a proprietary trunking mechanism. This mode could be used to support Lucent's *Open Trunk*, Cisco's *Fast EtherChannel* (FEC), and Cisco's *Gigabit EtherChannel* (GEC). In the static mode, as in generic link aggregation, the switch administrator needs to assign the ports to the team, and this assignment cannot be altered by the BASP, as there is no exchange of the Link Aggregation Control Protocol (LACP) frame.

With this mode, all adapters in the team are configured to receive packets for the same MAC address. Trunking operates on Layer 2 addresses and supports load balancing and failover for both inbound and outbound traffic. The BASP driver determines the load-balancing scheme for outbound packets, using Layer 4 protocols previously discussed, whereas the team link partner determines the load-balancing scheme for inbound packets.

The attached switch must support the appropriate trunking scheme for this mode of operation. Both the BASP and the switch continually monitor their ports for link loss. In the event of link loss on any port, traffic is automatically diverted to other ports in the team.

Network Communications

The following are the key attributes of Generic Static Trunking:

- **Failover mechanism** (link loss detection)
- **Load balancing algorithm.** Outbound traffic is balanced through Broadcom proprietary mechanism based L4 flows. Inbound traffic is balanced according to a switch specific mechanism.
- Outbound Load Balancing using MAC Address is not supported.
- **Outbound Load Balancing using IP address is supported.**
- **Multivendor teaming is supported** (must include at least one Broadcom Ethernet adapter as a team member)

Applications

Generic trunking works with switches that support Cisco Fast EtherChannel, Cisco Gigabit EtherChannel, Extreme Networks Load Sharing and Bay Networks or IEEE 802.3ad Link Aggregation static mode. Since load balancing is implemented on Layer 2 addresses, all higher protocols such as IP, IPX, and NetBEUI are supported. Therefore, this is the recommended teaming mode when the switch supports generic trunking modes over SLB.

Configuration Recommendations

Static trunking supports connecting the teamed ports to switches if they are on the same broadcast domain and support generic trunking. It does not support connecting to a router or Layer 3 switches since the ports must be on the same subnet.

Dynamic Trunking (IEEE 802.3ad Link Aggregation)

This mode supports link aggregation through static and dynamic configuration via the Link Aggregation Control Protocol (LACP). With this mode, all adapters in the team are configured to receive packets for the same MAC address. The MAC address of the first adapter in the team is used and cannot be substituted for a different MAC address. The BASP driver determines the load-balancing scheme for outbound packets, using Layer 4 protocols previously discussed, whereas the team's link partner determines the load-balancing scheme for inbound packets. Because the load balancing is implemented on Layer 2, all higher protocols such as IP, IPX, and NetBEUI are supported. The attached switch must support the 802.3ad Link Aggregation standard for this mode of operation. The switch manages the inbound traffic to the adapter while the BASP manages the outbound traffic. Both the BASP and the switch continually monitor their ports for link loss. In the event of link loss on any port, traffic is automatically diverted to other ports in the team.

Network Communications

The following are the key attributes of Dynamic Trunking:

- Failover mechanism – Link loss detection
- Load Balancing Algorithm – Outbound traffic is balanced through a Broadcom proprietary mechanism based on L4 flows. Inbound traffic is balanced according to a switch specific mechanism.
- Outbound Load Balancing using MAC Address - No
- Outbound Load Balancing using IP Address - Yes
- Multivendor teaming – Supported (must include at least one Broadcom Ethernet adapter as a team member)

Applications

Dynamic trunking works with switches that support IEEE 802.3ad Link Aggregation dynamic mode using LACP. Inbound load balancing is switch dependent. In general, the switch traffic is load balanced based on L2 addresses. In this case, all network protocols such as IP, IPX, and NetBEUI are load balanced. Therefore, this is the recommended teaming mode when the switch supports LACP, except when switch fault tolerance is required. SLB is the only teaming mode that supports switch fault tolerance.

Configuration Recommendations

Dynamic trunking supports connecting the teamed ports to switches as long as they are on the same broadcast domain and supports IEEE 802.3ad LACP trunking. It does not support connecting to a router or Layer 3 switches since the ports must be on the same subnet.

DRIVER SUPPORT BY OPERATING SYSTEM

As previously noted, BASP is supported in Windows Server 2008 and 2012 operating system environments. For Linux environments, Broadcom's Network Interface Card Extension (NICE) support is required. NICE is an extension provided by Broadcom to standard Linux drivers and supports monitoring of Address Resolution Protocol (ARP) requests, link detection, and VLANs.

The various teaming mode features are summarized in the table below.

Table 6.

Features	Windows Support
Smart Load Balancing™	
User interface	BACS[a]
Number of teams	4
Number of adapters per team	8
Hot replace	Yes
Hot add	Yes
Hot remove	Yes
Link speed support	Different speeds
Frame protocol	IP
Incoming packet management	BASP
Outgoing packet management	BASP
Failover event	Loss of link or LiveLink event
Failover time	<500 ms
Fallback time	1.5 s[b] (approximate)
LiveLink support	Yes
MAC address	Different
Multivendor teaming	Yes
Generic Trunking	
User interface	BACS
Number of teams	4
Number of adapters per team	8
Hot replace	Yes
Hot add	Yes
Hot remove	Yes
Link speed support	Different speeds
Frame protocol	All
Incoming packet management	Switch
Outgoing packet management	BASP
Failover event	Loss of link only
Failover time	500 ms
Fallback time	1.5 s[b] (approximate)
MAC address	Same for all adapters
Multivendor teaming	Yes

Table 6.

Features	Windows Support
Dynamic Trunking	
User interface	BACS
Number of teams	4
Number of adapters per team	8
Hot replace	Yes
Hot add	Yes
Hot remove	Yes
Link speed support	Different speeds
Frame protocol	All
Incoming packet management	Switch
Outgoing packet management	BASP
Failover event	Loss of link only
Failover time	<500 ms
Fallback time	1.5 s[b] (approximate)
MAC address	Same for all adapters
Multivendor teaming	Yes

[a] Broadcom Advanced Control Suite
[b] Make sure that Port Fast or Edge Port is enabled

Supported Teaming Speeds

The various link speeds that are supported for each type of team are listed in Table 7. Mixed speed refers to the capability of teaming adapters that are running at different link speeds.

Table 7. Link Speeds in Teaming

Type of Team	Link Speed	Traffic Direction	Speed Support
SLB	10/100/1000	Incoming/outgoing	Mixed speed
FEC	100	Incoming/outgoing	Same speed
GEC	1000	Incoming/outgoing	Same speed
IEEE 802.3ad	10/100/1000	Incoming/outgoing	Mixed speed

Teaming and Other Advanced Networking Properties

- Checksum Offload
- IEEE 802.1p QoS Tagging
- Large Send Offload
- Jumbo Frames
- IEEE 802.1Q VLANs
- Wake on LAN
- Preboot Execution Environment (PXE)

Before creating a team, adding or removing team members, or changing advanced settings of a team member, make sure each team member has been configured similarly. Settings to check include VLANs and QoS Packet Tagging, Jumbo Frames, and the various offloads. The advanced adapter properties and teaming support are listed in Table 8.

Table 8. Advanced Adapter Properties and Teaming Support

Adapter Property	Supported by Teamed Virtual Adapter
Checksum Offload	Yes
IEEE 802.1p QoS Tagging	No
Large Send Offload	Yes[a]
Jumbo Frames	Yes[b]
IEEE 802.1Q VLANs	Yes
Wake on LAN	No
Preboot Execution environment (PXE)	Yes[c]

[a] All adapters on the team must support this feature. Some adapters may not support this feature if ASF/IPMI is also enabled.
[b] Must be supported by all adapters in the team.
[c] As a PXE sever only, not as a client.

CHECKSUM OFFLOAD

Checksum Offload is a property of the Broadcom network adapters that allows the TCP/IP/UDP checksums for send and receive traffic to be calculated by the adapter hardware rather than by the host CPU. In high-traffic situations, this can allow a system to handle more connections more efficiently than if the host CPU were forced to calculate the checksums. This property is inherently a hardware property and would not benefit from a software-only implementation. An adapter that supports Checksum Offload advertises this capability to the operating system so that the checksum does not need to be calculated in the protocol stack; because the intermediate driver is located directly between the protocol layer and the miniport driver, the protocol layer is not able to offload any checksums. Checksum Offload is only supported for IPv4 at this time.

IEEE 802.1P QOS TAGGING

The IEEE 802.1p standard includes a 3-bit field (supporting a maximum of 8 priority levels), which allows for traffic prioritization. The BASP intermediate driver does not support IEEE 802.1p QoS tagging.

LARGE SEND OFFLOAD

Large Send Offload (LSO) is a feature provided by Broadcom network adapters that prevents an upper level protocol such as TCP from breaking a large data packet into a series of smaller packets with headers appended to them. The protocol stack need only generate a single header for a data packet as large as 64 KB, and the adapter hardware breaks the data buffer into appropriately-sized Ethernet frames with the correctly sequenced header (based on the single header originally provided).

JUMBO FRAMES

The use of jumbo frames was originally proposed by Alteon Networks, Inc. in 1998 and increased the maximum size of an Ethernet frame to a maximum size of 9000 bytes. Though never formally adopted by the IEEE 802.3 Working Group, support for jumbo frames has been implemented in Broadcom adapters. The BASP intermediate driver supports jumbo frames, provided that all of the physical adapters in the team also support jumbo frames and the same size is set on all adapters in the team.

IEEE 802.1Q VLANS

In 1998, the IEEE approved the 802.3ac standard, which defines frame format extensions to support Virtual Bridged Local Area Network tagging on Ethernet networks as specified in the IEEE 802.1Q specification. The VLAN protocol permits insertion of a tag into an Ethernet frame to identify the VLAN to which a frame belongs. If present, the 4-byte VLAN tag is inserted into the Ethernet frame between the source MAC address and the length/type field. The first 2-bytes of the VLAN tag consist of the IEEE 802.1Q tag type, whereas the second 2 bytes include a user priority field and the VLAN identifier (VID). Virtual LANs (VLANs) allow the user to split the physical LAN into logical subparts. Each defined VLAN behaves as its own separate network, with its traffic and broadcasts isolated from the others, thus increasing bandwidth efficiency within each logical group. VLANs also enable the administrator to enforce appropriate security and quality of service (QoS) policies. The BASP supports the creation of 64 VLANs per team or adapter: 63 tagged and 1 untagged. The operating system and system resources, however, limit the actual number of VLANs. VLAN support is provided according to IEEE 802.1q and is supported in a teaming environment as well as on a single adapter. Note that VLANs are supported only with homogeneous teaming and not in a multivendor teaming environment. The BASP intermediate driver supports VLAN tagging. One or more VLANs may be bound to a single instance of the intermediate driver.

WAKE ON LAN

Wake on LAN (WOL) is a feature that allows a system to be awakened from a sleep state by the arrival of a specific packet over the Ethernet interface. Because a virtual adapter is implemented as a software only device, it lacks the hardware features to implement Wake on LAN and cannot be enabled to wake the system from a sleeping state via the virtual adapter. The physical adapters, however, support this property, even when the adapter is part of a team.

PREBOOT EXECUTION ENVIRONMENT (PXE)

The Preboot Execution Environment (PXE) allows a system to boot from an operating system image over the network. By definition, PXE is invoked before an operating system is loaded, so there is no opportunity for the BASP intermediate driver to load and enable a team. As a result, teaming is not supported as a PXE client, though a physical adapter that participates in a team when the operating system is loaded may be used as a PXE client. Whereas a teamed adapter cannot be used as a PXE client, it can be used for a PXE server, which provides operating system images to PXE clients using a combination of Dynamic Host Control Protocol (DHCP) and the Trivial File Transfer Protocol (TFTP). Both of these protocols operate over IP and are supported by all teaming modes.

GENERAL NETWORK CONSIDERATIONS

TEAMING ACROSS SWITCHES

SLB teaming can be configured across switches. The switches, however, must be connected together. Generic Trunking and Link Aggregation do not work across switches because each of these implementations requires that all physical adapters in a team share the same Ethernet MAC address. It is important to note that SLB can only detect the loss of link between the ports in the team and their immediate link partner. SLB has no way of reacting to other hardware failures in the switches and cannot detect loss of link on other ports.

Switch-Link Fault Tolerance

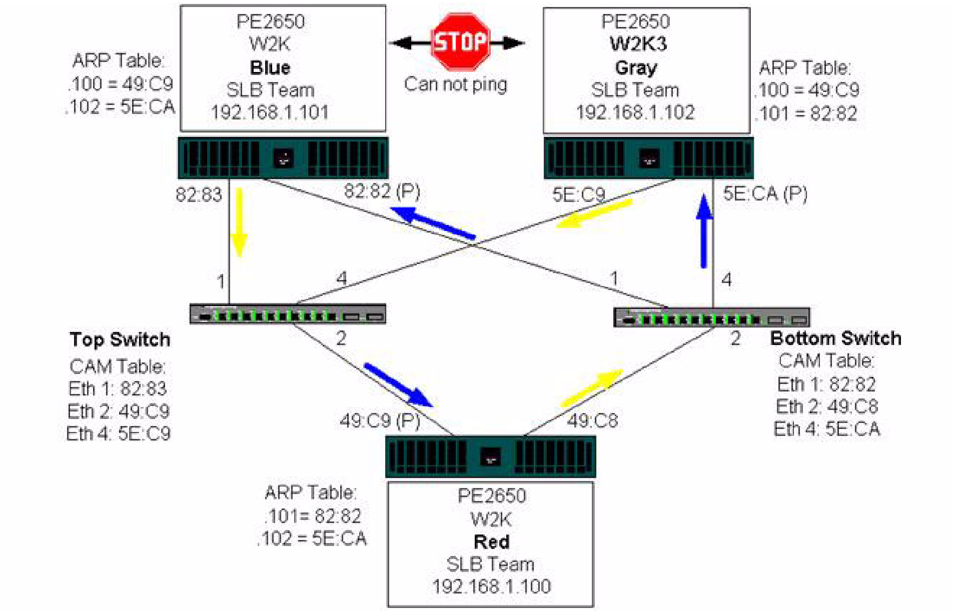
The diagrams below describe the operation of an SLB team in a switch fault tolerant configuration. We show the mapping of the ping request and ping replies in an SLB team with two active members. All servers (Blue, Gray and Red) have a continuous ping to each other.Figure 3 is a setup without the interconnect cable in place between the two switches. Figure 4 has the interconnect cable in place, and Figure 5 is an example of a failover event with the Interconnect cable in place. These scenarios describe the behavior of teaming across the two switches and the importance of the interconnect link.

The diagrams show the secondary team member sending the ICMP echo requests (yellow arrows) while the primary team member receives the respective ICMP echo replies (blue arrows). This illustrates a key characteristic of the teaming software. The load balancing algorithms do not synchronize how frames are load balanced when sent or received. In other words, frames for a given conversation can go out and be received on different interfaces in the team. This is true for all types of teaming supported by Broadcom. Therefore, an interconnect link must be provided between the switches that connect to ports in the same team.

In the configuration without the interconnect, an ICMP Request from Blue to Gray goes out port 82:83 destined for Gray port 5E:CA, but the Top Switch has no way to send it there because it cannot go along the 5E:C9 port on Gray. A similar scenario occurs when Gray attempts to ping Blue. An ICMP Request goes out on 5E:C9 destined for Blue 82:82, but cannot get there. Top Switch does not have an entry for 82:82 in its CAM table because there is no interconnect between the two switches. Pings, however, flow between Red and Blue and between Red and Gray.

Furthermore, a failover event would cause additional loss of connectivity. Consider a cable disconnect on the Top Switch port 4. In this case, Gray would send the ICMP Request to Red 49:C9, but because the Bottom switch has no entry for 49:C9 in its CAM Table, the frame is flooded to all its ports but cannot find a way to get to 49:C9.

Figure 3. Teaming Across Switches Without an Interswitch Link



The addition of a link between the switches allows traffic from/to Blue and Gray to reach each other without any problems. Note the additional entries in the CAM table for both switches. The link interconnect is critical for the proper operation of the team. As a result, it is highly advisable to have a link aggregation trunk to interconnect the two switches to ensure high availability for the connection.

Figure 4. Teaming Across Switches With Interconnect

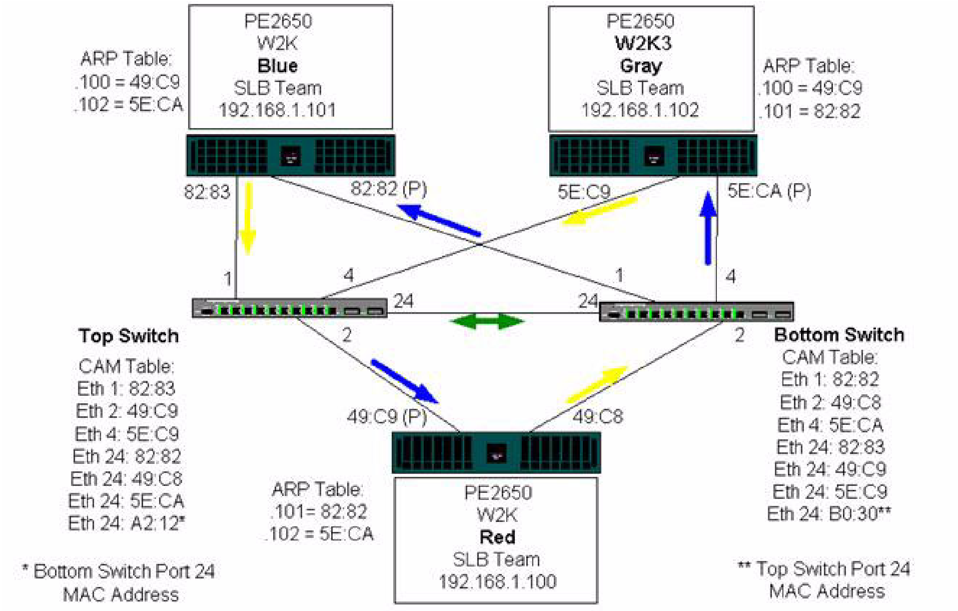
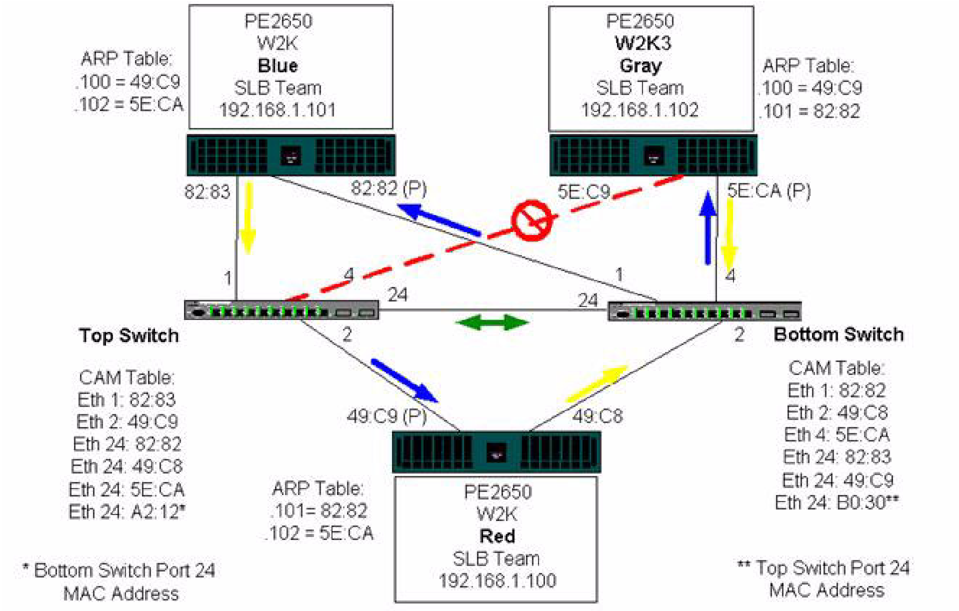


Figure 5 represents a failover event in which the cable is unplugged on the Top Switch port 4. This is a successful failover with all stations pinging each other without loss of connectivity.

Figure 5. Failover Event



Spanning Tree Algorithm

- Topology Change Notice (TCN)
- Port Fast/Edge Port

In Ethernet networks, only one active path may exist between any two bridges or switches. Multiple active paths between switches can cause loops in the network. When loops occur, some switches recognize stations on both sides of the switch. This situation causes the forwarding algorithm to malfunction allowing duplicate frames to be forwarded. Spanning tree algorithms provide path redundancy by defining a tree that spans all of the switches in an extended network and then forces certain redundant data paths into a standby (blocked) state. At regular intervals, the switches in the network send and receive spanning tree packets that they use to identify the path. If one network segment becomes unreachable, or if spanning tree costs change, the spanning tree algorithm reconfigures the spanning tree topology and re-establishes the link by activating the standby path. Spanning tree operation is transparent to end stations, which do not detect whether they are connected to a single LAN segment or a switched LAN of multiple segments.

Spanning Tree Protocol (STP) is a Layer 2 protocol designed to run on bridges and switches. The specification for STP is defined in IEEE 802.1d. The main purpose of STP is to ensure that you do not run into a loop situation when you have redundant paths in your network. STP detects/disables network loops and provides backup links between switches or bridges. It allows the device to interact with other STP compliant devices in your network to ensure that only one path exists between any two stations on the network.

After a stable network topology has been established, all bridges listen for hello BPDUs (Bridge Protocol Data Units) transmitted from the root bridge. If a bridge does not get a hello BPDU after a predefined interval (Max Age), the bridge assumes that the link to the root bridge is down. This bridge then initiates negotiations with other bridges to reconfigure the network to re-establish a valid network topology. The process to create a new topology can take up to 50 seconds. During this time, end-to-end communications are interrupted.

The use of Spanning Tree is not recommended for ports that are connected to end stations, because by definition, an end station does not create a loop within an Ethernet segment. Additionally, when a teamed adapter is connected to a port with Spanning Tree enabled, users may experience unexpected connectivity problems. For example, consider a teamed adapter that has a lost link on one of its physical adapters. If the physical adapter were to be reconnected (also known as fallback), the intermediate driver would detect that the link has been reestablished and would begin to pass traffic through the port. Traffic would be lost if the port was temporarily blocked by the Spanning Tree Protocol.

Topology Change Notice (TCN)

A bridge/switch creates a forwarding table of MAC addresses and port numbers by learning the source MAC address that received on a particular port. The table is used to forward frames to a specific port rather than flooding the frame to all ports. The typical maximum aging time of entries in the table is 5 minutes. Only when a host has been silent for 5 minutes would its entry be removed from the table. It is sometimes beneficial to reduce the aging time. One example is when a forwarding link goes to blocking and a different link goes from blocking to forwarding. This change could take up to 50 seconds. At the end of the STP re-calculation a new path would be available for communications between end stations. However, because the forwarding table would still have entries based on the old topology, communications may not be reestablished until after 5 minutes when the affected ports entries are removed from the table. Traffic would then be flooded to all ports and re-learned. In this case it is beneficial to reduce the aging time. This is the purpose of a topology change notice (TCN) BPDU. The TCN is sent from the affected bridge/switch to the root bridge/switch. As soon as a bridge/switch detects a topology change (a link going down or a port going to forwarding) it sends a TCN to the root bridge via its root port. The root bridge then advertises a BPDU with a Topology Change to the entire network.This causes every bridge to reduce the MAC table aging time to 15 seconds for a specified amount of time. This allows the switch to re-learn the MAC addresses as soon as STP re-converges.

Topology Change Notice BPDUs are sent when a port that was forwarding changes to blocking or transitions to forwarding. A TCN BPDU does not initiate an STP recalculation. It only affects the aging time of the forwarding table entries in the switch.It will not change the topology of the network or create loops. End nodes such as servers or clients trigger a topology change when they power off and then power back on.

Port Fast/Edge Port

To reduce the effect of TCNs on the network (for example, increasing flooding on switch ports), end nodes that are powered on/off often should use the Port Fast or Edge Port setting on the switch port they are attached to. Port Fast or Edge Port is a command that is applied to specific ports and has the following effects:

- Ports coming from link down to link up will be put in the forwarding STP mode instead of going from listening to learning and then to forwarding. STP is still running on these ports.
- The switch does not generate a Topology Change Notice when the port is going up or down.

Layer 3 Routing/Switching

The switch that the teamed ports are connected to must not be a Layer 3 switch or router. The ports in the team must be in the same network.

Teaming with Hubs (for troubleshooting purposes only)

- Hub Usage in Teaming Network Configurations

- SLB Teams
- SLB Team Connected to a Single Hub
- Generic and Dynamic Trunking (FEC/GEC/IEEE 802.3ad)

SLB teaming can be used with 10/100 hubs, but it is only recommended for troubleshooting purposes, such as connecting a network analyzer in the event that switch port mirroring is not an option.

Hub Usage in Teaming Network Configurations

Although the use of hubs in network topologies is functional in some situations, it is important to consider the throughput ramifications when doing so. Network hubs have a maximum of 100 Mbps half-duplex link speed, which severely degrades performance in either a Gigabit or 100 Mbps switched-network configuration. Hub bandwidth is shared among all connected devices; as a result, when more devices are connected to the hub, the bandwidth available to any single device connected to the hub is reduced in direct proportion to the number of devices connected to the hub.

It is not recommended to connect team members to hubs; only switches should be used to connect to teamed ports. An SLB team, however, can be connected directly to a hub for troubleshooting purposes. Other team types can result in a loss of connectivity if specific failures occur and should not be used with hubs.

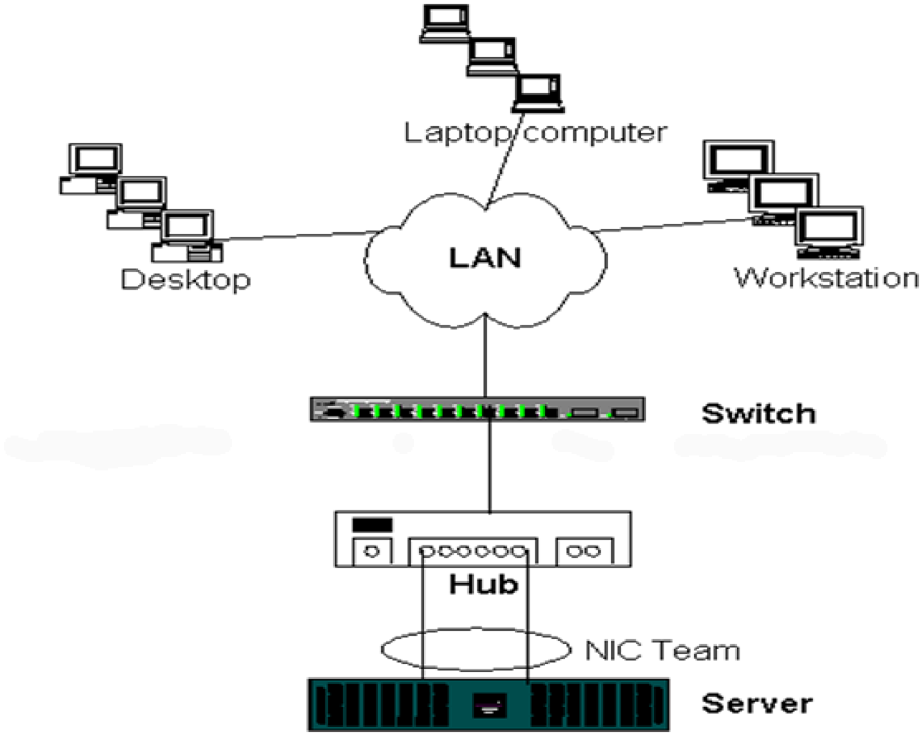
SLB Teams

SLB teams are the only teaming type not dependant on switch configuration. The server intermediate driver handles the load balancing and fault tolerance mechanisms with no assistance from the switch. These elements of SLB make it the only team type that maintains failover and fallback characteristics when team ports are connected directly to a hub.

SLB Team Connected to a Single Hub

SLB teams configured as shown in Figure97 maintain their fault tolerance properties. Either server connection could potentially fail, and network functionality is maintained. Clients could be connected directly to the hub, and fault tolerance would still be maintained; server performance, however, would be degraded.

Figure 6. Team Connected to a Single Hub



Generic and Dynamic Trunking (FEC/GEC/IEEE 802.3ad)

FEC/GEC and IEEE 802.3ad teams cannot be connected to any hub configuration. These team types must be connected to a switch that has also been configured for this team type.

TEAMING WITH MICROSOFT NLB/WLBS

The SLB mode of teaming *does not* work in Microsoft's Network Load Balancing (NLB) unicast mode, only in multicast mode. Due to the mechanism used by the NLB service, the recommended teaming configuration in this environment is Failover (SLB with a standby NIC) as load balancing is managed by NLB.

APPLICATION CONSIDERATIONS

TEAMING AND CLUSTERING

Microsoft Cluster Software

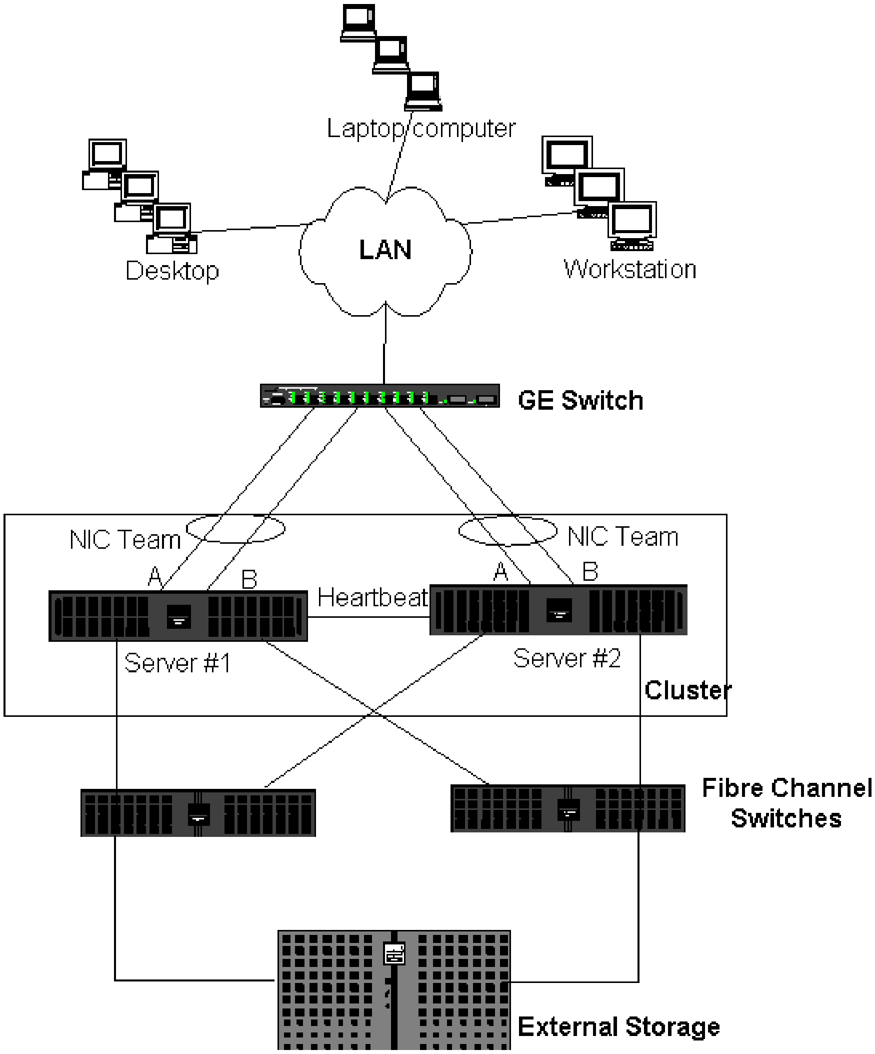
In each cluster node, it is strongly recommended that customers install at least two network adapters (on-board adapters are acceptable). These interfaces serve two purposes. One adapter is used exclusively for intra-cluster *heartbeat* communications. This is referred to as the *private adapter* and usually resides on a separate private subnetwork. The other adapter is used for client communications and is referred to as the *public adapter*.

Multiple adapters may be used for each of these purposes: private, intracluster communications and public, external client communications. All Broadcom teaming modes are supported with Microsoft Cluster Software for the public adapter only. Private network adapter teaming is not supported. Microsoft indicates that the use of teaming on the private interconnect of a server cluster is not supported because of delays that could possibly occur in the transmission and receipt of heartbeat packets between the nodes. For best results, when you want redundancy for the private interconnect, disable teaming and use the available ports to form a second private interconnect. This achieves the same end result and provides dual, robust communication paths for the nodes to communicate over.

For teaming in a clustered environment, customers are recommended to use the same brand of adapters.

Figure 7 shows a 2-node Fibre-Channel cluster with three network interfaces per cluster node: one private and two public. On each node, the two public adapters are teamed, and the private adapter is not. Teaming is supported across the same switch or across two switches. Figure 8 shows the same 2-node Fibre-Channel cluster in this configuration.

Figure 7. Clustering With Teaming Across One Switch



NOTE: Microsoft Network Load Balancing is not supported with Microsoft Cluster Software.

High-Performance Computing Cluster

Gigabit Ethernet is typically used for the following three purposes in high-performance computing cluster (HPCC) applications:

1. Inter-Process Communications (IPC): For applications that do not require low-latency high-bandwidth interconnects (such as Myrinet, InfiniBand), Gigabit Ethernet can be used for communication between the compute nodes.
2. I/O: Ethernet can be used for file sharing and serving the data to the compute nodes. This can be done simply using an

NFS server or using parallel file systems such as PVFS.

3. Management & Administration: Ethernet is used for out-of-band (ERA) and in-band (OMSA) management of the nodes in the cluster. It can also be used for job scheduling and monitoring.

In our current HPCC offerings, only one of the on-board adapters is used. If Myrinet or IB is present, this adapter serves I/O and administration purposes; otherwise, it is also responsible for IPC. In case of an adapter failure, the administrator can use the Felix package to easily configure adapter 2. Adapter teaming on the host side is neither tested nor supported in HPCC.

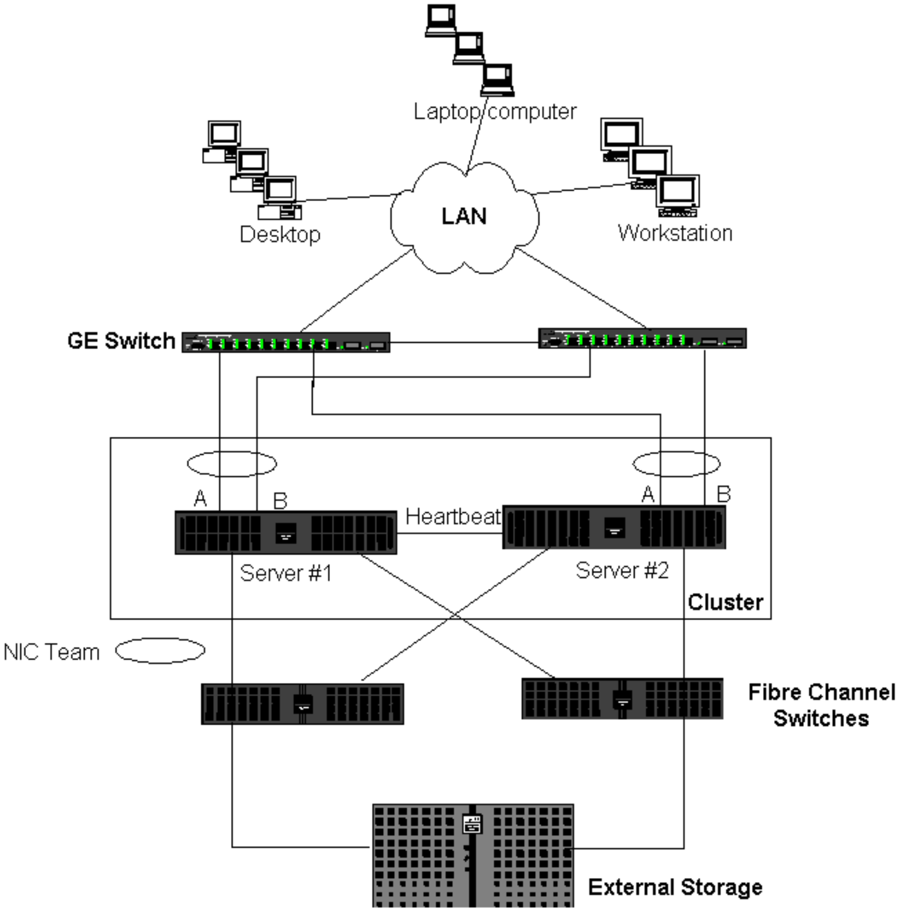
Advanced Features

PXE is used extensively for the deployment of the cluster (installation and recovery of compute nodes). Teaming is typically not used on the host side and it is not a part of our standard offering. Link aggregation is commonly used between switches, especially for large configurations. Jumbo frames, although not a part of our standard offering, may provide performance improvement for some applications due to reduced CPU overhead.

Oracle

In our Oracle Solution Stacks, we support adapter teaming in both the private network (interconnect between RAC nodes) and public network with clients or the application layer above the database layer.

Figure 8. Clustering With Teaming Across Two Switches

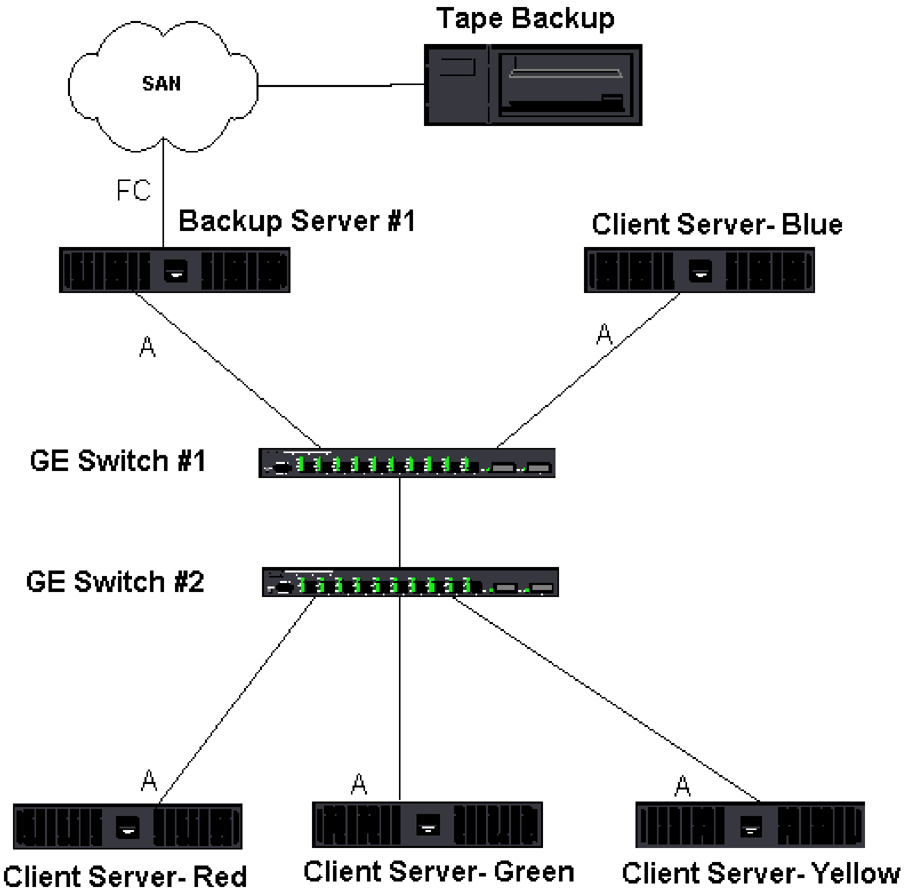


Teaming and Network Backup

- Load Balancing and Failover
- Fault Tolerance

When you perform network backups in a nonteamed environment, overall throughput on a backup server adapter can be easily impacted due to excessive traffic and adapter overloading. Depending on the number of backup servers, data streams, and tape drive speed, backup traffic can easily consume a high percentage of the network link bandwidth, thus impacting production data and tape backup performance. Network backups usually consist of a dedicated backup server running with tape backup software such as NetBackup, Galaxy or Backup Exec. Attached to the backup server is either a direct SCSI tape backup unit or a tape library connected through a fiber channel storage area network (SAN). Systems that are backed up over the network are typically called clients or remote servers and usually have a tape backup software agent installed. Figure 9 shows a typical 1 Gbps nonteamed network environment with tape backup implementation.

Figure 9. Network Backup without Teaming



Because there are four client servers, the backup server can simultaneously stream four backup jobs (one per client) to a multidrive autoloader. Because of the single link between the switch and the backup server, however, a 4-stream backup can easily saturate the adapter and link. If the adapter on the backup server operates at 1 Gbps (125 MB/s), and each client is able to stream data at 20 MB/s during tape backup, the throughput between the backup server and switch will be at 80 MB/s (20 MB/s x 4), which is equivalent to 64% of the network bandwidth. Although this is well within the network bandwidth range, the 64% constitutes a high percentage, especially if other applications share the same link.

Load Balancing and Failover

As the number of backup streams increases, the overall throughput increases. Each data stream, however, may not be able to maintain the same performance as a single backup stream of 25 MB/s. In other words, even though a backup server can stream data from a single client at 25 MB/s, it is not expected that four simultaneously running backup jobs will stream at 100 MB/s (25 MB/s x 4 streams). Although overall throughput increases as the number of backup streams increases, each backup stream can be impacted by tape software or network stack limitations.

For a tape backup server to reliably use adapter performance and network bandwidth when backing up clients, a network infrastructure must implement teaming such as load balancing and fault tolerance. Data centers will incorporate redundant switches, link aggregation, and trunking as part of their fault tolerant solution. Although teaming device drivers will manipulate the way data flows through teamed interfaces and failover paths, this is transparent to tape backup applications and does not interrupt any tape backup process when backing up remote systems over the network. Figure 10 shows a network topology that demonstrates tape backup in a Broadcom teamed environment and how smart load balancing can *load balance* tape backup data across teamed adapters.

There are four paths that the client-server can use to send data to the backup server, but only one of these paths will be designated during data transfer. One possible path that Client-Server Red can use to send data to the backup server is:

Example Path: Client-Server Red sends data through Adapter A, Switch 1, Backup Server Adapter A.

The designated path is determined by two factors:

1. Client-Server ARP cache; which points to the backup server MAC address. This is determined by the Broadcom intermediate driver inbound load balancing algorithm.
2. The physical adapter interface on Client-Server Red will be used to transmit the data. The Broadcom intermediate driver outbound load balancing algorithm determines this (see Outbound Traffic Flow and Inbound Traffic Flow (SLB Only)).

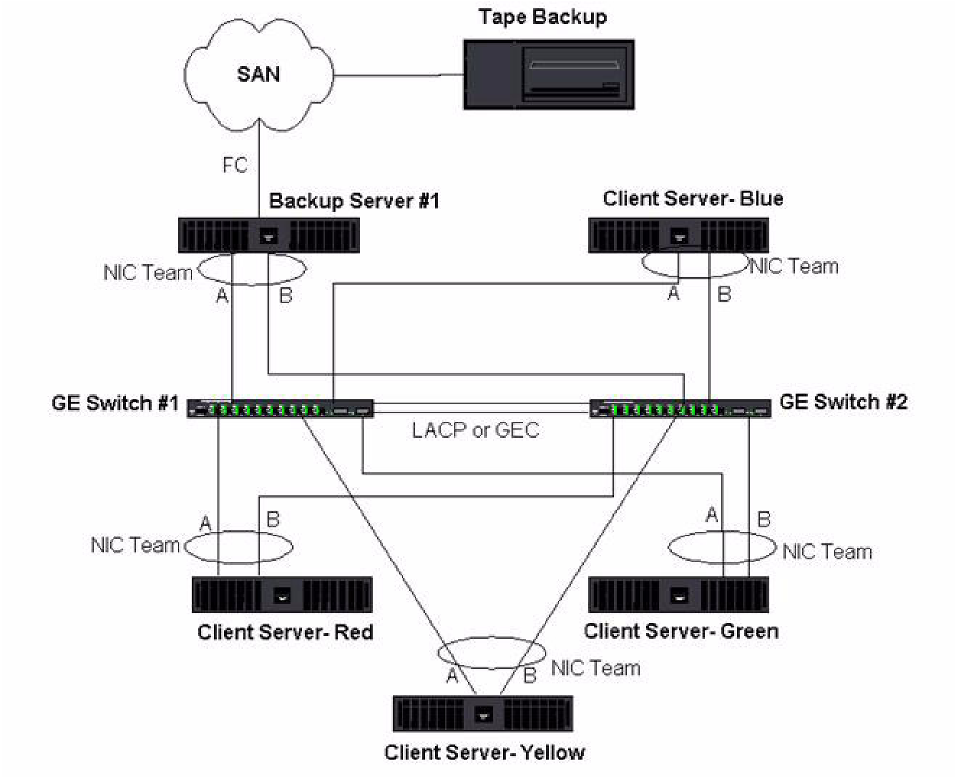
The teamed interface on the backup server transmits a gratuitous address resolution protocol (G-ARP) to Client-Server Red, which in turn, causes the client server ARP cache to get updated with the Backup Server MAC address. The load balancing mechanism within the teamed interface determines the MAC address embedded in the G-ARP. The selected MAC address is essentially the destination for data transfer from the client server. On Client-Server Red, the SLB teaming algorithm will determine which of the two adapter interfaces will be used to transmit data. In this example, data from Client-Server Red is received on the backup server Adapter A interface. To demonstrate the SLB mechanisms when additional load is placed on the teamed interface, consider the scenario when the backup server initiates a second backup operation: one to Client-Server Red, and one to Client-Server Blue. The route that Client-Server Blue uses to send data to the backup server is dependant on its ARP cache, which points to the backup server MAC address. Because Adapter A of the backup server is already under load from its backup operation with Client-Server Red, the backup server invokes its SLB algorithm to *inform* Client-Server Blue (thru an G-ARP) to update its ARP cache to reflect the backup server Adapter B MAC address. When Client-Server Blue needs to transmit data, it uses either one of its adapter interfaces, which is determined by its own SLB algorithm. What is important is that data from Client-Server Blue is received by the Backup Server Adapter B interface, and not by its Adapter A interface. This is important because with both backup streams running simultaneously, the backup server must *load balance* data streams from different clients. With both backup streams running, each adapter interface on the backup server is processing an equal load, thus load-balancing data across both adapter interfaces.

The same algorithm applies if a third and fourth backup operation is initiated from the backup server. The teamed interface on the backup server transmits a unicast G-ARP to backup clients to inform them to update their ARP cache. Each client then transmits backup data along a route to the target MAC address on the backup server.

Fault Tolerance

If a network link fails during tape backup operations, all traffic between the backup server and client stops and backup jobs fail. If, however, the network topology was configured for both Broadcom SLB and switch fault tolerance, then this would allow tape backup operations to continue without interruption during the link failure. All failover processes within the network are transparent to tape backup software applications. To understand how backup data streams are directed during network failover process, consider the topology in Figure 8. Client-Server Red is transmitting data to the backup server through Path 1, but a link failure occurs between the backup server and the switch. Because the data can no longer be sent from Switch #1 to the Adapter A interface on the backup server, the data is redirected from Switch #1 through Switch #2, to the Adapter B interface on the backup server. This occurs without the knowledge of the backup application because all fault tolerant operations are handled by the adapter team interface and trunk settings on the switches. From the client server perspective, it still operates as if it is transmitting data through the original path.

Figure 10. Network Backup With SLB Teaming Across Two Switches



TROUBLESHOOTING TEAMING PROBLEMS

- Teaming Configuration Tips
- Troubleshooting Guidelines

When running a protocol analyzer over a virtual adapter teamed interface, the MAC address shown in the transmitted frames may not be correct. The analyzer does not show the frames as constructed by BASP and shows the MAC address of the team and not the MAC address of the interface transmitting the frame. It is suggested to use the following process to monitor a team:

1. Mirror all uplink ports from the team at the switch.
2. If the team spans two switches, mirror the interlink trunk as well.
3. Sample all mirror ports independently.
4. On the analyzer, use an adapter and driver that does not filter QoS and VLAN information.

TEAMING CONFIGURATION TIPS

When troubleshooting network connectivity or teaming functionality issues, ensure that the following information is true for your configuration.

1. Although mixed speed SLB teaming is supported, it is recommended that all adapters in a team be the same speed (either all Gigabit Ethernet or all Fast Ethernet).
2. If LiveLink is not enabled, disable Spanning Tree Protocol or enable an STP mode that bypasses the initial phases (for example, Port Fast, Edge Port) for the switch ports connected to a team.
3. All switches that the team is directly connected to must have the same hardware revision, firmware revision, and software revision to be supported.
4. To be teamed, adapters should be members of the same VLAN. In the event that multiple teams are configured, each team should be on a separate network.
5. Do not enter a multicast or broadcast address in the Locally Administered Address field.
6. Do not assign a Locally Administered Address on any physical adapter that is a member of a team.
7. Verify that power management is disabled on all physical members of any team (the **Allow the computer to turn off this device to save power** box on the **Power Management** tab in adapter **Properties** should be cleared—see Setting Power Management Options in “Windows Driver Software”).
8. Remove any static IP address from the individual physical team members before the team is built.
9. A team that requires maximum throughput should use LACP or GEC\FEC. In these cases, the intermediate driver is only responsible for the outbound load balancing while the switch performs the inbound load balancing.
10. Aggregated teams (802.3ad \ LACP and GEC\FEC) must be connected to only a single switch that supports IEEE 802.3a, LACP or GEC/FEC.
11. It is not recommended to connect any team to a hub, as a hub only support half duplex. Hubs should be connected to a team for troubleshooting purposes only. Disabling the device driver of a network adapter participating in an LACP or GEC/FEC team may have adverse affects with network connectivity. Broadcom recommends that the adapter first be physically disconnected from the switch before disabling the device driver in order to avoid a network connection loss.
12. Verify the base (Miniport) and team (intermediate) drivers are from the same release package. The mixing of base and teaming drivers from different CD releases is not supported.
13. Test the connectivity to each physical adapter prior to teaming.

14. Test the failover and fallback behavior of the team before placing into a production environment.
15. When moving from a nonproduction network to a production network, it is strongly recommended to test again for failover and fallback.
16. Test the performance behavior of the team before placing it into a production environment.

TROUBLESHOOTING GUIDELINES

Before you call for support, make sure you have completed the following steps for troubleshooting network connectivity problems when the server is using adapter teaming.

1. Make sure the link light is ON for every adapter and all the cables are attached.
2. Check that the matching base and intermediate drivers belong to the same release and are loaded correctly.
3. Check for a valid IP address using the **ipconfig** command for Windows.
4. Check that STP is disabled or Edge Port/Port Fast is enabled on the switch ports connected to the team or that LiveLink is being used.
5. Check that the adapters and the switch are configured identically for link speed and duplex.
6. If possible, break the team and check for connectivity to each adapter independently to confirm that the problem is directly associated with teaming.
7. Check that all switch ports connected to the team are on the same VLAN.
8. Check that the switch ports are configured properly for Generic Trunking (FEC/GEC)/802.3ad-Draft Static type of teaming and that it matches the adapter teaming type. If the system is configured for an SLB type of team, make sure the corresponding switch ports *are not* configured for Generic Trunking (FEC/GEC)/802.3ad-Draft Static types of teams.

FREQUENTLY ASKED QUESTIONS

Question: Under what circumstances is traffic not load balanced? Why is all traffic not load balanced evenly across the team members?

Answer: The bulk of traffic does not use IP/TCP/UDP or the bulk of the clients are in a different network. The receive load balancing is not a function of traffic load, but a function of the number of clients that are connected to the system.

Question: What network protocols are load balanced when in a team?

Answer: Broadcom's teaming software only supports IP/TCP/UDP traffic. All other traffic is forwarded to the primary adapter.

Question: Which protocols are load balanced with SLB and which ones are not?

Answer: Only IP/TCP/UDP protocols are load balanced in both directions: send and receive. IPX is load balanced on the transmit traffic only.

Question: Can I team a port running at 100 Mbps with a port running at 1000 Mbps?

Answer: Mixing link speeds within a team is only supported for Smart Load Balancing™ teams and 802.3ad teams, as stated earlier.

Question: Can I team a fiber adapter with a copper Gigabit Ethernet adapter?

Answer: Yes with SLB, and yes if the switch allows for it in FEC/GEC and 802.3ad.

Question: What is the difference between adapter load balancing and Microsoft's Network Load Balancing (NLB)?

Answer: Adapter load balancing is done at a network session level, whereas NLB is done at the system application level.

Question: Can I connect the teamed adapters to a hub?

Answer: Yes. Teamed ports can be connected to a hub for troubleshooting purposes. However, this practice is not recommended for normal operation because the performance would be degraded due to hub limitations. Connect the teamed ports to a switch instead.

Question: Can I connect the teamed adapters to ports in a router?

Answer: No. All ports in a team must be on the same network; in a router, however, each port is a separate network by definition. All teaming modes require that the link partner be a Layer 2 switch.

Question: Can I use teaming with Microsoft Cluster Services?

Answer: Yes. Teaming is supported on the public network only, not on the private network used for the heartbeat link.

Question: Can PXE work over a virtual adapter (team)?

Answer: A PXE client operates in an environment before the operating system is loaded; as a result, virtual adapters have not been enabled yet. If the physical adapter supports PXE, then it can be used as a PXE client, whether or not it is part of a virtual adapter when the operating system loads. PXE servers may operate over a virtual adapter.

Question: Can WOL work over a virtual adapter (team)?

Answer: Wake-on-LAN functionality operates in an environment before the operating system is loaded. WOL occurs when the system is off or in standby, so no team is configured.

Question: What is the maximum number of ports that can be teamed together?

Answer: Up to 8 ports can be assigned to a team.

Question: What is the maximum number of teams that can be configured on the same system?

Answer: Up to 4 teams can be configured on the same system.

Question: Why does my team lose connectivity for the first 30 to 50 seconds after the primary adapter is restored (fallback)?

Answer: Because Spanning Tree Protocol is bringing the port from blocking to forwarding. You must enable Port Fast or Edge Port on the switch ports connected to the team or use LiveLink to account for the STP delay.

Question: Can I connect a team across multiple switches?

Answer: Smart Load Balancing can be used with multiple switches because each physical adapter in the system uses a unique Ethernet MAC address. Link Aggregation and Generic Trunking cannot operate across switches because they require all physical adapters to share the same Ethernet MAC address.

Question: How do I upgrade the intermediate driver (BASP)?

Answer: The intermediate driver cannot be upgraded through the Local Area Connection Properties. It must be upgraded using the Setup installer.

Question: How can I determine the performance statistics on a virtual adapter (team)?

Answer: In Broadcom Advanced Control Suite, click the BASP Statistics tab for the virtual adapter.

Question: Can I configure NLB and teaming concurrently?

Answer: Yes, but only when running NLB in a multicast mode (NLB is not supported with MS Cluster Services).

Question: Should both the backup system and client systems that are backed up be teamed?

Answer: Because the backup system is under the most data load, it should always be teamed for link aggregation and failover. A fully redundant network, however, requires that both the switches and the backup clients be teamed for fault tolerance and link aggregation.

Question: During backup operations, does the adapter teaming algorithm load balance data at a byte-level or a session-level?

Answer: When using adapter teaming, data is only load balanced at a session level and not a byte level to prevent out-of-order frames. Adapter teaming load balancing does not work the same way as other storage load balancing mechanisms such as EMC PowerPath.

Question: Is there any special configuration required in the tape backup software or hardware to work with adapter teaming?

Answer: No special configuration is required in the tape software to work with teaming. Teaming is transparent to tape backup applications.

Question: How do I know what driver I am currently using?

Answer: In all operating systems, the most accurate method for checking the driver revision is to physically locate the driver file and check the properties.

Question: Can SLB detect a switch failure in a Switch Fault Tolerance configuration?

Answer: No. SLB can detect only the loss of link between the teamed port and its immediate link partner. SLB cannot detect link failures on other ports. For more information, see LiveLink™ Functionality.

Question: Where can I get the latest supported drivers?

Answer: Go to Broadcom support at http://www.broadcom.com/support/ethernet_nic/downloaddrivers.php for driver package updates or support documents.

Question: Where do I monitor real time statistics for an adapter team in a Windows system?

Answer: Use the Broadcom Advanced Control Suite (BACS) to monitor general, IEEE 802.3, and custom counters.

EVENT LOG MESSAGES

- Windows System Event Log Messages
- Base Driver (Physical Adapter/Miniport)
- Intermediate Driver (Virtual Adapter/Team)

WINDOWS SYSTEM EVENT LOG MESSAGES

The known base driver and intermediate driver Windows System Event Log status messages for the Broadcom NetXtreme Gigabit Ethernet adapters as of December 2004 are listed. As a Broadcom adapter driver loads, Windows places a status code in the system event viewer. There may be up to two classes of entries for these event codes depending on whether both drivers are loaded (one set for the base or miniport driver and one set for the intermediate or teaming driver).

Base Driver (Physical Adapter/Miniport)

Table 9 lists the event log messages supported by the base driver, explains the cause for the message, and provides the recommended action.

Table 9. Base Driver Event Log Messages

Message Number	Message	Cause	Corrective Action
1	Failed to allocate memory for the device block. Check system memory resource usage.	The driver cannot allocate memory from the operating system.	Close running applications to free memory.
2	Failed to allocate map registers	The driver cannot allocate map registers from the operating system.	Unload other drivers that may allocate map registers.
3	Failed to access configuration information. Reinstall the network driver.	The driver cannot access PCI configuration space registers on the adapter.	For add-in adapters: reseat the adapter in the slot, move the adapter to another PCI slot, or replace the adapter.
4	The network link is down. Check to make sure the network cable is properly connected.	The adapter has lost its connection with its link partner.	Check that the network cable is connected, verify that the network cable is the right type, and verify that the link partner (for example, switch or hub) is working correctly.
5	The network link is up.	The adapter has established a link.	Informational message only. No action is required.
6	Network controller configured for 10Mb half-duplex link.	The adapter has been manually configured for the selected line speed and duplex settings.	Informational message only. No action is required.
7	Network controller configured for 10Mb full-duplex link.	The adapter has been manually configured for the selected line speed and duplex settings.	Informational message only. No action is required.
8	Network controller configured for 100Mb half-duplex link.	The adapter has been manually configured for the selected line speed and duplex settings.	Informational message only. No action is required.
9	Network controller configured for 100Mb full-duplex link.	The adapter has been manually configured for the selected line speed and duplex settings.	Informational message only. No action is required.
10	Network controller configured for 1Gb half-duplex link.	The adapter has been manually configured for the selected line speed and duplex settings.	Informational message only. No action is required.
11	Network controller configured for 1Gb full-duplex link.	The adapter has been manually configured for the selected line speed and duplex settings.	Informational message only. No action is required.
12	Medium not supported.	The operating system does not support the IEEE 802.3 medium.	Reboot the operating system, run a virus check, run a disk check (chkdsk), and reinstall the operating system.

Table 9. Base Driver Event Log Messages (Cont.)

Message Number	Message	Cause	Corrective Action
13	Unable to register the interrupt service routine.	The device driver cannot install the interrupt handler.	Reboot the operating system; remove other device drivers that may be sharing the same IRQ.
14	Unable to map IO space.	The device driver cannot allocate memory-mapped I/O to access driver registers.	Remove other adapters from the system, reduce the amount of physical memory installed, and replace the adapter.
15	Driver initialized successfully.	The driver has successfully loaded.	Informational message only. No action is required.
16	NDIS is resetting the miniport driver.	The NDIS layer has detected a problem sending/ receiving packets and is resetting the driver to resolve the problem.	Run Broadcom Advanced Control Suite diagnostics; check that the network cable is good.
17	Unknown PHY detected. Using a default PHY initialization routine.	The driver could not read the PHY ID.	Replace the adapter.
18	This driver does not support this device. Upgrade to the latest driver.	The driver does not recognize the installed adapter.	Upgrade to a driver version that supports this adapter.
19	Driver initialization failed.	Unspecified failure during driver initialization.	Reinstall the driver, update to a newer driver, run Broadcom Advanced Control Suite diagnostics, or replace the adapter.

Intermediate Driver (Virtual Adapter/Team)

Table 10 lists the event log messages supported by the intermediate driver, explains the cause for the message, and provides the recommended action.

Table 10. Intermediate Driver Event Log Messages

System Event Message Number	Message	Cause	Corrective Action
1	Unable to register with NDIS.	The driver cannot register with the NDIS interface.	Unload other NDIS drivers.
2	Unable to instantiate the management interface.	The driver cannot create a device instance.	Reboot the operating system.
3	Unable to create symbolic link for the management interface.	Another driver has created a conflicting device name.	Unload the conflicting device driver that uses the name *Blf*.
4	Broadcom Advanced Server Program Driver has started.	Another driver has created a conflicting device name.	Informational message only. No action is required.
5	Broadcom Advanced Server Program Driver has stopped.	The driver has stopped.	Informational message only. No action is required.
6	Could not allocate memory for internal data structures.	The driver cannot allocate memory from the operating system.	Close running applications to free memory
7	Could not bind to adapter.	The driver could not open one of the team physical adapters.	Unload and reload the physical adapter driver, install an updated physical adapter driver, or replace the physical adapter.
8	Successfully bind to adapter.	The driver successfully opened the physical adapter.	Informational message only. No action is required.
9	Network adapter is disconnected.	The physical adapter is not connected to the network (it has not established link).	Check that the network cable is connected, verify that the network cable is the right type, and verify that the link partner (switch or hub) is working correctly.
10	Network adapter is connected.	The physical adapter is connected to the network (it has established link).	Informational message only. No action is required.
11	Broadcom Advanced Program Features Driver is not designed to run on this version of Operating System.	The driver does not support the operating system on which it is installed.	Consult the driver release notes and install the driver on a supported operating system or update the driver.
12	Hot-standby adapter is selected as the primary adapter for a team without a load balancing adapter.	A standby adapter has been activated.	Replace the failed physical adapter.
13	Network adapter does not support Advanced Failover.	The physical adapter does not support the Broadcom NIC Extension (NICE).	Replace the adapter with one that does support NICE.
14	Network adapter is enabled via management interface.	The driver has successfully enabled a physical adapter through the management interface.	Informational message only. No action is required.

Table 10. Intermediate Driver Event Log Messages (Cont.)

System Event Message Number	Message	Cause	Corrective Action
15	Network adapter is disabled via management interface.	The driver has successfully disabled a physical adapter through the management interface.	Informational message only. No action is required.
16	Network adapter is activated and is participating in network traffic.	A physical adapter has been added to or activated in a team.	Informational message only. No action is required.
17	Network adapter is de-activated and is no longer participating in network traffic.	The driver does not recognize the installed adapter.	Informational message only. No action is required.

Virtual LANs: Broadcom NetXtreme 57XX User Guide

VLAN Overview

Virtual LANs (VLANs) allow you to split your physical LAN into logical parts, to create logical segmentation of workgroups, and to enforce security policies for each logical segment. Each defined VLAN behaves as its own separate network with its traffic and broadcasts isolated from the others, increasing bandwidth efficiency within each logical group. Up to 64 VLANs (63 tagged and 1 untagged) can be defined for each Broadcom adapter on your server, depending on the amount of memory available in your system.

VLANs can be added to a team to allow multiple VLANs with different VLAN IDs. A virtual adapter is created for each VLAN added.

Although VLANs are commonly used to create individual broadcast domains and/or separate IP subnets, it is sometimes useful for a server to have a presence on more than one VLAN simultaneously. Broadcom adapters support multiple VLANs on a per-port or per-team basis, allowing very flexible network configurations.

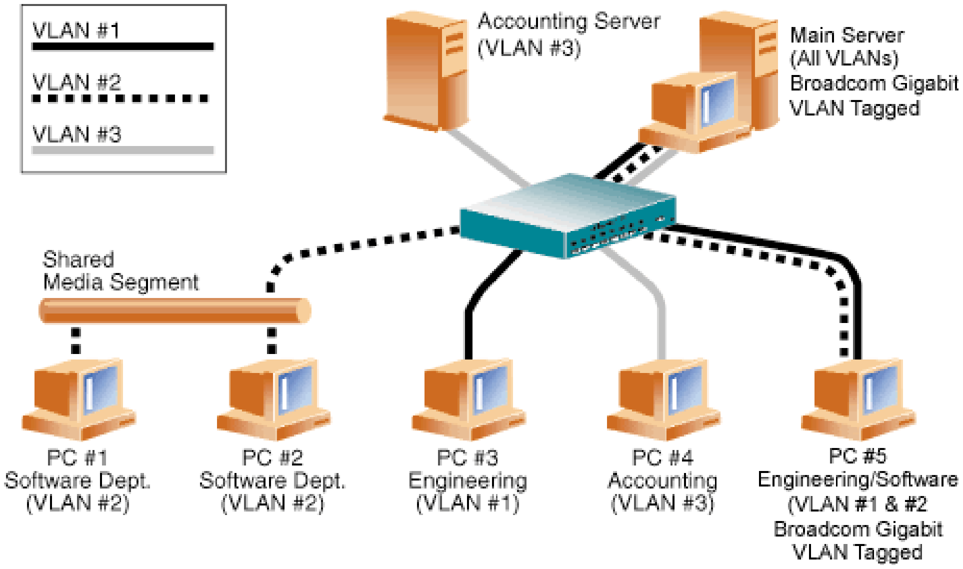

VLAN #1
VLAN #2
VLAN #3
Accounting Server (VLAN #3)
Main Server (All VLANs) Broadcom Gigabit VLAN Tagged
Shared Media Segment
PC #1 Software Dept. (VLAN #2)
PC #2 Software Dept. (VLAN #2)
PC #3 Engineering (VLAN #1)
PC #4 Accounting (VLAN #3)
PC #5 Engineering/Software (VLAN #1 & #2 Broadcom Gigabit VLAN Tagged

Figure 1: Example of Servers Supporting Multiple VLANs with Tagging

Figure 1 shows an example network that uses VLANs. In this example network, the physical LAN consists of a switch, two servers, and five clients. The LAN is logically organized into three different VLANs, each representing a different IP subnet. The features of this network are described in Table 1:

Table 1: Example VLAN Network Topology

Component	***Description***
VLAN #1	An IP subnet consisting of the Main Server, PC #3, and PC #5. This subnet represents an engineering group.
VLAN #2	Includes the Main Server, PCs #1 and #2 via shared media segment, and PC #5. This VLAN is a software development group.
VLAN #3	Includes the Main Server, the Accounting Server and PC #4. This VLAN is an accounting group.
Main Server	A high-use server that needs to be accessed from all VLANs and IP subnets. The Main Server has a Broadcom adapter installed. All three IP subnets are accessed via the single physical adapter interface. The server is attached to one of the switch ports, which is configured for VLANs #1, #2, and #3. Both the adapter and the connected switch port have tagging turned on. Because of the tagging VLAN capabilities of both devices, the server is able to communicate on all three IP subnets in this network, but continues to maintain broadcast separation between all of them.
Accounting Server	Available to VLAN #3 only. The Accounting Server is isolated from all traffic on VLANs #1 and #2. The switch port connected to the server has tagging turned off.
PCs #1 and #2	Attached to a shared media hub that is then connected to the switch. PCs #1 and #2 belong to VLAN #2 only, and are logically in the same IP subnet as the Main Server and PC #5. The switch port connected to this segment has tagging turned off.
PC #3	A member of VLAN #1, PC #3 can communicate only with the Main Server and PC #5. Tagging is not enabled on PC #3 switch port.
PC #4	A member of VLAN #3, PC #4 can only communicate with the servers. Tagging is not enabled on PC #4 switch port.
PC #5	A member of both VLANs #1 and #2, PC #5 has an Broadcom adapter installed. It is connected to switch port #10. Both the adapter and the switch port are configured for VLANs #1 and #2 and have tagging enabled.

NOTE: VLAN tagging is only required to be enabled on switch ports that create trunk links to other switches, or on ports connected to tag-capable end-stations, such as servers or workstations with Broadcom adapters.

Adding VLANs to Teams

Each team supports up to 64 VLANs (63 tagged and 1 untagged). Note that only Broadcom adapters and Alteon® AceNIC adapters can be part of a team with VLANs. With multiple VLANs on an adapter, a server with a single adapter can have a logical presence on multiple IP subnets. With multiple VLANs in a team, a server can have a logical presence on multiple IP subnets and benefit from load balancing and failover. For instructions on adding a VLAN to a team, see Adding a VLAN for Windows operating systems.

NOTE: Adapters that are members of a failover team can also be configured to support VLANs. Because VLANs are not supported for an Intel LOM, if an Intel LOM is a member of a failover team, VLANs cannot be configured for that team.

Manageability: Broadcom NetXtreme 57XX User Guide

- CIM
- SNMP

CIM

The Common Information Model (CIM) is an industry standard defined by the Distributed Management Task Force (DMTF). Microsoft implements CIM on Windows platforms such as Windows Server 2008. Broadcom will support CIM on Windows Server 2008 platforms.

Broadcom's implementation of CIM will provide various classes to provide information to users through CIM client applications. Note that Broadcom CIM data provider will provide data only, and users can choose their preferred CIM client software to browse the information exposed by Broadcom CIM provider.

Broadcom CIM provider provides information through BRCM_NetworkAdapter and BRCM_ExtraCapacityGroup classes. BRCM_NetworkAdapter class provides network adapter information pertaining to a group of adapters, including both Broadcom and other vendors' controllers. BRCM_ExtraCapacityGroup class provides team configuration for the Broadcom Advanced Server Program (BASP) Program. Current implementation will provide team information and information of physical network adapters in the team.

Broadcom Advanced Server Program provides events through event logs. Users can use the "Event Viewer" provided by Windows Server 2008, or use CIM to inspect or monitor these events. Broadcom CIM provider will also provide event information through the CIM generic event model. These events are __InstanceCreationEvent, __InstanceDeletionEvent and __InstanceModificationEvent, and are defined by CIM. CIM requires the client application to register the events from the client application using queries, as examples shown below in order to receive events properly.

```
SELECT * FROM __InstanceModificationEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceModificationEvent
where TargetInstance ISA "BRCM_ExtraCapacityGroup"
SELECT * FROM __InstanceCreationEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceDeletionEvent
where TargetInstance ISA "BRCM_NetworkAdapter"
SELECT * FROM __InstanceCreationEvent
where TargetInstance ISA "BRCM_ActsAsSpare"
SELECT * FROM __InstanceDeletionEvent
where TargetInstance ISA "BRCM_ActsAsSpare"
```

For detailed information about these events, see the CIM documentation at http://www.dmtf.org/standards/published_documents/DSP0004V2.3_final.pdf.

SNMP

BASP Subagent

The BASP subagent, baspmgnt.dll, is designed for Windows Server 2008 SNMP service. It is required to install the SNMP service before installing the BASP subagent.

The BASP subagent allows an SNMP manager software to actively monitor the configurations and performance of the Broadcom Advanced Server features. The subagent also provides an alarm trap to an SNMP manager to inform the manager of any changes to the conditions of the BASP component.

The BASP subagent allows monitoring of the configurations and statistics for the BASP teams, the physical NIC adapters participating in a team, and the virtual NIC adapters created as the result of teaming. Non-teamed NIC adapters are not monitored at this time. The BASP configuration data includes information such as team IDs, physical/virtual/VLAN/team adapter IDs, physical/virtual/VLAN/team/ adapter descriptions, and MAC addresses of the adapters.

The statistics include detailed information such as data packets transmitted and received for the physical/virtual/VLAN/team adapters.

The alarm trap forwards information about the changes in configuration of the physical adapters participating in a team, such as physical adapter link up/down, and adapter installed/removed events.

To monitor this information, an SNMP manager must load the Broadcom BASP MIB database files to allow monitoring of the information described above. These files, which are shown below, are included with the installation CD:

baspcfg.mib

baspstat.mib

basptrap.mib

BASP Extensible-Agent

The Broadcom NetXtreme Gigabit Ethernet Controller Extended Information SNMP extensible-agent, bcmif.dll, is designed for Windows Server 2008 SNMP service.

The extensible-agent allows the SNMP manager software to actively monitor the configurations of the Broadcom NetXtreme adapter. It is intended to supplement the information already provided by the standard SNMP Management Network Interface information.

The extensible-agent provides in-depth information about a Broadcom NetXtreme adapter such as:

- MAC address
- Bound IP address
- IP subnet mask
- Physical link status
- Adapter state
- Line speed
- Duplex mode
- Memory range
- Interrupt setting

- Bus number
- Device number
- Function number

To monitor this information, a SNMP manager needs to load the Broadcom Extended information MIB file to allow monitoring of the information described above. This file, bcmif.mib, is included on the Broadcom NetXtreme adapter installation CD.

The monitored workstation requires the installation of the Broadcom Extended Information SNMP extensible-agent, bcmif.dll, and requires the Microsoft Windows Server 2008 SNMP service to be installed and loaded.

Installing the Hardware: Broadcom NetXtreme 57XX User Guide

NOTE: This section applies only to add-in NIC models of Broadcom NetXtreme Gigabit Ethernet adapters.

SYSTEM REQUIREMENTS

Before you install the Broadcom NetXtreme Gigabit Ethernet adapter, verify that your system meets the requirements listed for your operating system:

HARDWARE REQUIREMENTS

- Pentium-based system that meets operating system requirements
- One open 32-bit or 64-bit PCI and/or PCI Express slot
- 128-MB RAM (minimum) for Windows and Linux.

OPERATING SYSTEM REQUIREMENTS

General

- PCI v2.3 33/66 MHz Bus Interface (BCM5701/BCM5703)
- PCI-X v1.0 64-bit 100-MHz Bus Interface (BCM5701 only)
- PCI-X v1.0 64-bit 133-MHz Bus Interface (BCM5703 only)
- PCI Express v1.0a, x1 (or greater) Host Interface (BCM5721)

Microsoft Windows

One of the following versions of Microsoft Windows:

- Windows Server 2012
- Windows Server 2008 Family

Linux

NOTE: The current version of the adapter driver has been tested on the latest Red Hat, SuSE, and other Linux distributions for i386, ia64, and x86_64 CPU architectures using 2.4.x and 2.6.x kernels. The driver has been tested up to kernel version 2.4.33 and 2.6.13. The driver should work on other little endian or big endian CPU architectures, but only very limited testing has been done on some of these machines. The Makefile may have to be modified to include architecture-specific compile switches, and some minor changes in the source files may also be required. On these machines, patching the driver into the kernel is recommended.

Safety Precautions

CAUTION! The adapter is being installed in a system that operates with voltages that can be lethal. Before you remove the cover of your system, you must observe the following precautions to protect yourself and to prevent damage to the system components:

- Remove any metallic objects or jewelry from your hands and wrists.
- Make sure to use only insulated or nonconducting tools.
- Verify that the system is powered OFF and unplugged before you touch internal components.
- Install or remove adapters in a static-free environment. The use of a properly grounded wrist strap or other personal antistatic devices and an antistatic mat is strongly recommended.

Preinstallation Checklist

1. Verify that your server meets the hardware and software requirements listed under System Requirements.
2. Verify that your server is using the latest BIOS.

NOTE: If you acquired the adapter software on a floppy disk or from the Broadcom support website (http://www.broadcom.com/support/ethernet_nic/downloaddrivers.php), verify the path to the adapter driver files.

3. If your system is active, shut it down.
4. When system shutdown is complete, turn off the power and unplug the power cord.
5. Holding the adapter card by the edges, remove it from its shipping package and place it on an antistatic surface.
6. Check the adapter for visible signs of damage, particularly on the card edge connector. Never attempt to install any damaged adapter.

INSTALLING THE ADAPTER

The following instructions apply to installing the Broadcom NetXtreme Gigabit Ethernet adapter (add-in NIC) in most servers. Refer to the manuals that were supplied with your server for details about performing these tasks on your particular server.

1. Review the Safety Precautions and Preinstallation Checklist. Before installing the adapter, ensure the system power is OFF and unplugged from the power outlet, and that proper electrical grounding procedures have been followed.
2. Open the system case, and select any empty PCI/PCI-X/PCI Express slot. If you do not know how to identify any of these PCI slots, refer to your system documentation.
3. Remove the blank cover-plate from the slot that you selected.
4. Align the adapter connector edge with the connector slot in the system.
5. Applying even pressure at both corners of the card, push the adapter card into the slot until it is firmly seated. When the adapter is properly seated, the adapter port connectors are aligned with the slot opening, and the adapter faceplate is flush against the system chassis.

⚠

CAUTION! Do not use excessive force when seating the card as this may damage the system or the adapter. If you have difficulty seating the adapter, remove it, realign it, and try again.

6. Secure the adapter with the adapter clip or screw.
7. Close the system case and disconnect any personal antistatic devices.

CONNECTING THE NETWORK CABLES

COPPER

The Broadcom NetXtreme Gigabit Ethernet adapter has one RJ-45 connector used for attaching the system to an Ethernet copper-wire segment.

NOTE: The Broadcom NetXtreme Gigabit Ethernet adapter supports Automatic MDI Crossover (MDIX), which eliminates the need for crossover cables when connecting machines back-to-back. A straight-through Category 5 cable allows the machines to communicate when connected directly together.

1. Select an appropriate cable. Table 1: “10/100/1000BASE-T Cable Specifications” lists the cable requirements for connecting to 10/100/1000BASE-T ports:

Table 1: 10/100/1000BASE-T Cable Specifications

Port Type	***Connector***	***Media***	***Maximum Distance***
10BASE-T	RJ-45	Category 3, 4, or 5 UTP	100 meters (328 feet)
100/1000BASE-T[1]	RJ-45	Category 5[2] UTP	100 meters (328 feet)

Table 1: 10/100/1000BASE-T Cable Specifications

Port Type	*Connector*	*Media*	*Maximum Distance*

[1] 1000BASE-T signaling requires four twisted pairs of Category 5 balanced cabling, as specified in ISO/IEC 11801:1995 and EIA/TIA-568-A (1995) and tested using procedures defined in TIA/EIA TSB95.

[2] Category 5 is the minimum requirement. Category 5e and Category 6 are fully supported.

2. Connect one end of the cable to the adapter.
3. Connect the other end of the cable to an RJ-45 Ethernet network port.

NOTE: After the cable is properly connected at both ends, the port LEDs on the adapter should be functional. See Table 1: "10/100/1000BASE-T Cable Specifications," on page 66 for a description of network link and activity indications

Creating a Driver Disk: Broadcom NetXtreme 57XX User Guide

Create driver disks using the Broadcom MakeDisk utility (Setup.exe file). This utility runs under Windows and allows you to create disks with the following drivers:

- Windows 2000
- Windows Server 2003 (IA32, IA64, X64 (AMD64))

To create a driver disk or file

1. Insert a 3.5-inch disk into drive A (default) or create a folder on your hard disk.
2. Insert the installation CD into your system CD-ROM drive.
3. If the CD does not automatically run, then browse to the MakeDisk folder on the CD and double-click **Setup.exe**.
4. Follow the onscreen instructions.
5. Select the driver or drivers of choice. Note that selecting multiple drivers results in creating multiple disks.
6. Click **Next**.
7. Click **OK**.
8. If more than one driver was selected, **Setup Needs the Next Disk** is displayed again. Insert another 3.5-inch disk or browse to another folder and click **OK**.

When all driver disks have been created, an information screen is displayed confirming that the disks were successfully created. Click **OK**.

Broadcom Boot Agent Driver Software: Broadcom NetXtreme 57XX User Guide

Overview

Broadcom NetXtreme Gigabit Ethernet adapters support Preboot Execution Environment (PXE), Remote Program Load (RPL), and Bootstrap Protocol (BootP). Multi-Boot Agent (MBA) is a software module that allows your networked system to boot with the images provided by remote systems across the network. The Broadcom MBA driver complies with the PXE 2.1 specification and is released with both monolithic and split binary images. This provides flexibility to users in different environments where the motherboard may or may not have built-in base code.

The MBA module operates in a client/system environment. A network consists of one or more boot systems that provide boot images to multiple systems through the network. The Broadcom implementation of the MBA module has been tested successfully in the following environments:

- **Linux® Red Hat® PXE Server.** Broadcom PXE clients are able to remotely boot and use network resources (NFS mount, and so forth) and to perform Linux installations. In the case of a remote boot, the Linux universal driver binds seamlessly with the Broadcom Universal Network Driver Interface (UNDI) and provides a network interface in the Linux remotely-booted client environment.
- **Intel® APITEST.** The Broadcom PXE driver passes all API compliance test suites.
- **MS-DOS UNDI.** The MS-DOS Universal Network Driver Interface (UNDI) seamlessly binds with the Broadcom UNDI to provide a network device driver interface specification (NDIS2) interface to the upper layer protocol stack. This allows systems to connect to network resources in an MS-DOS environment.
- **Remote Installation Service (RIS)**. The Broadcom PXE clients are able to remotely boot to a Windows Server 2008 system running RIS to initialize and install Windows Server 2008 and prior operating systems.
- **Windows Deployment Service (WDS)**. For Windows Server 2003 SP2, RIS was replaced by WDS, which offers a Broadcom PXE client to install Windows operating systems, including Windows Server 2008.

Setting Up MBA in a Client Environment

Use the following procedure for add-in NICs. For LOMs, refer to your computer's system guide.

Setting up MBA in a client environment involves the following steps:

1. Enabling the MBA driver.
2. Configuring the MBA driver.
3. Setting up the BIOS for the boot order.

Enabling the MBA Driver

To enable or disable the MBA driver:

1. Insert the driver source media in the CD-ROM drive and boot up in DOS mode.
2. Type:
   ```
   drive:\dos\utility
   ```
   where

   `drive` is the drive letter of the CD-ROM drive.

   NOTE: The B57udiag.exe file is on the installation CD.
3. Type:
   ```
   b57udiag -mba [ 0-disable | 1-enable ] -c devnum
   ```
   where

   `devnum` is the specific device(s) number (0,1,2, …) to be programmed.

Specifying the MBA Protocol

To specify the MBA protocol:

1. Place the driver source media in the CD-ROM drive and boot up in DOS mode.
2. Type:
   ```
   drive:\dos\utility
   ```
   where

   `drive` is the drive letter of the CD-ROM drive.
3. Type:
   ```
   b57udiag -mbap [ 0-pxe | 1-rpl | 2-bootp ] -c devnum
   ```
   where

   `devnum` is the specific device(s) number (0,1,2,...) to be programmed.

Forcing the MBA to a Specific Speed

To force the MBA to a specific speed

1. Place the driver source media in the CD-ROM drive and boot up in DOS mode.
2. Type:

```
drive:\dos\utility
```

where

`drive` is the drive letter of the CD-ROM drive.

3. Type:
   ```
   b57udiag -mbas [ 0-Auto | 1-10HD | 2-10FD | 3-100H | 4-100F ] -c devnum
   ```
   where

   `devnum` is the specific device(s) number (0,1,2,...) to be programmed.

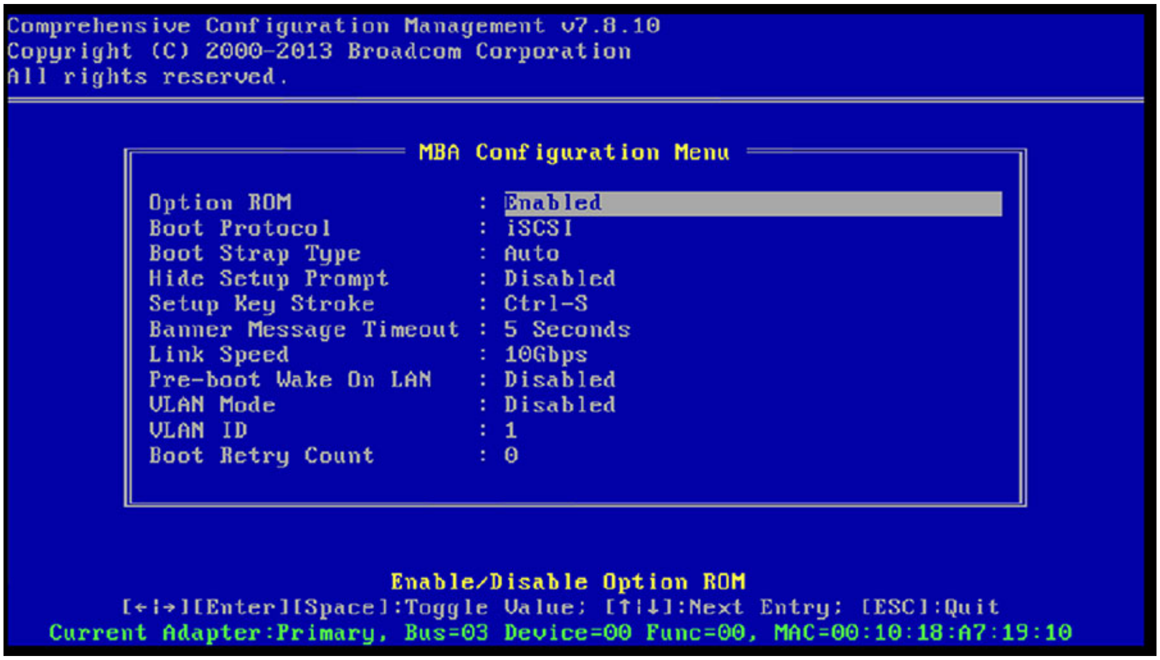
Configuring the MBA Driver

This section pertains to configuring the MBA driver on add-in NIC models of the Broadcom network adapter. For configuring the MBA driver on LOM models of the Broadcom network adapter, check your system documentation.

1. Insert the installation CD in the CD-ROM drive and boot up in DOS mode.

Using CCM

1. Restart your system.
2. Press **CTRL+s** within 4 seconds after you are prompted to do so. A list of adapters displays.
   a. Select the adapter to configure and press **Enter**. The Main Menu displays.
   b. Select **MBA Configuration** to display the MBA Configuration menu.



```
Comprehensive Configuration Management v7.8.10
Copyright (C) 2000-2013 Broadcom Corporation
All rights reserved.

                    MBA Configuration Menu

     Option ROM                : Enabled
     Boot Protocol             : iSCSI
     Boot Strap Type           : Auto
     Hide Setup Prompt         : Disabled
     Setup Key Stroke          : Ctrl-S
     Banner Message Timeout    : 5 Seconds
     Link Speed                : 10Gbps
     Pre-boot Wake On LAN      : Disabled
     VLAN Mode                 : Disabled
     VLAN ID                   : 1
     Boot Retry Count          : 0

                   Enable/Disable Option ROM
     [←|→][Enter][Space]:Toggle Value; [↑|↓]:Next Entry; [ESC]:Quit
  Current Adapter:Primary, Bus=03 Device=00 Func=00, MAC=00:10:18:A7:19:10
```

3. Use the UP ARROW and DOWN ARROW keys to move to the Boot Protocol menu item. Then use the RIGHT ARROW or LEFT ARROW key to select the boot protocol of choice if other boot protocols besides Preboot Execution Environment (PXE) are available. If available, other boot protocols include Remote Program Load (RPL) and Bootstrap Protocol (BOOTP).

NOTE: If you have multiple adapters in your system and you are unsure which adapter you are configuring, press **CTRL+F6**, which causes the port LEDs on the adapter to start blinking.

4. Use the UP ARROW, DOWN ARROW, LEFT ARROW, and RIGHT ARROW keys to move to and change the values for other menu items, as desired.
5. Press **F4** to save your settings.
6. Press **ESC** when you are finished.

Using uEFI

1. Restart your system.
2. Enter the System Setup or Device Setting configuration menu.
3. Select the device on which you want to change MBA settings.
4. Select **MBA Configuration Menu**.
5. Use the drop-down menu to select the boot protocol of choice, if boot protocols other than Preboot Execution Environment (PXE) are available. If available, other boot protocols include iSCSI and Bootstrap Protocol (BOOTP).

> **NOTE:** For iSCSI boot-capable LOMs, the boot protocol is set via the BIOS. See your system documentation formore information.

6. Use the UP ARROW, DOWN ARROW, LEFT ARROW, and RIGHT ARROW keys to move to and change the values for other menu items, as desired.
7. Select **Back** to go to Main menu
8. Select **Finish** to save and exit.

Setting Up the BIOS

To boot from the network with the MBA, make the MBA enabled adapter the first bootable device under the BIOS. This procedure depends on the system BIOS implementation. Refer to the user manual for the system for instructions.

SETTING UP MBA IN A SERVER ENVIRONMENT

Linux Red Hat PXE Server

The Red Hat Enterprise Linux has PXE Server support. It allows users to remotely perform a complete Linux installation over the network. The distribution comes with the boot images boot kernel (vmlinuz) and initial ram disk (initrd), which are located on the Red Hat disk#1:

/images/pxeboot/vmlinuz

/images/pxeboot/initrd.img

Refer to the Red Hat documentation for instructions on how to install PXE Server on Linux.

The Initrd.img file distributed with Red Hat 8.0, however, does not have a Linux network driver for the Broadcom NetXtreme Gigabit Ethernet adapter.

This version requires drivers that are not part of the standard distribution. You can create a driver disk for the Broadcom NetXtreme Gigabit Ethernet adapter using files obtained from the support website.NetXtreme Refer to the Linux Readme.txt file for more information.

A remote boot does not require a standard Linux network driver for the Broadcom NetXtreme Gigabit Ethernet adapter. After the PXE client downloads the Linux kernel and initial ram disk, the Linux universal driver that came with the Linux distribution binds with the UNDI code of the PXE to form a Linux network driver.

NOTE: Refer to the Distrib.txt file on the installation CD for a list of the specific Linux distributions on which the driver has been tested.

DOS UNDI/Intel APITEST

To boot in DOS mode and connect to a network for the DOS environment, download the Intel PXE PDK from the Intel website. This PXE PDK comes with a TFTP/ProxyDHCP/Boot server. The PXE PDK can be downloaded from Intel at http://downloadcenter.intel.com/default.aspx.

iSCSI Protocol: Broadcom NetXtreme 57XX User Guide

iSCSI Boot

Broadcom NetXtreme Gigabit Ethernet adapters support iSCSI boot to enable network boot of operating systems to diskless systems. The iSCSI boot allows a Windows or Linux operating system boot from an iSCSI target machine located remotely over a standard IP network.

Supported Operating Systems for iSCSI Boot

The Broadcom NetXtreme Gigabit Ethernet adapters support iSCSI boot on the following operating systems:

- Windows Server 2012 64-bit
- Windows Server 2008 R2 64-bit
- Windows Server 2008 32-bit and 64-bit
- Windows Server 2012 64-bit
- Linux RHEL 5.5 and later, SLES 11.1 and later
- SLES 10.x and SLES 11

iSCSI Boot Setup

The iSCSI boot setup consists of:

- Configuring the iSCSI Target
- Configuring iSCSI Boot Parameters
- Preparing the iSCSI Boot Image
- Booting

Configuring the iSCSI Target

Configuring the iSCSI target varies by target vendors. For information on configuring the iSCSI target, refer to the documentation provided by the vendor. The general steps include:

1. Create an iSCSI target.
2. Create a virtual disk.
3. Map the virtual disk to the iSCSI target created in step 1.
4. Associate an iSCSI initiator with the iSCSI target.
5. Record the iSCSI target name, TCP port number, iSCSI Logical Unit Number (LUN), initiator Internet Qualified Name (IQN), and CHAP authentication details.

6. After configuring the iSCSI target, obtain the following:
   - Target IQN
   - Target IP address
   - Target TCP port number
   - Target LUN
   - Initiator IQN
   - CHAP ID and secret

Configuring iSCSI Boot Parameters

Configure the Broadcom iSCSI boot software for either static or dynamic configuration. Refer to Table 1 for configuration options available from the General Parameters screen.

Table 1 lists parameters for both IPv4 and IPv6. Parameters specific to either IPv4 or IPv6 are noted.

NOTE: Availability of IPv6 iSCSI boot is platform/device dependent.

Table 1: Configuration Options

Option	***Description***
TCP/IP parameters via DHCP	This option is specific to IPv4. Controls whether the iSCSI boot host software acquires the IP address information using DHCP (Enabled) or use a static IP configuration (Disabled).
IP Autoconfiguration	This option is specific to IPv6. Controls whether the iSCSI boot host software will configure a stateless link-local address and/or stateful address if DHCPv6 is present and used (Enabled). Router Solicit packets are sent out up to three times with 4 second intervals in between each retry. Or use a static IP configuration (Disabled).
iSCSI parameters via DHCP	Controls whether the iSCSI boot host software acquires its iSCSI target parameters using DHCP (Enabled) or through a static configuration (Disabled). The static information is entered through the iSCSI Initiator Parameters Configuration screen.
CHAP Authentication	Controls whether the iSCSI boot host software uses CHAP authentication when connecting to the iSCSI target. If CHAP Authentication is enabled, the CHAP ID and CHAP Secret are entered through the iSCSI Initiator Parameters Configuration screen.
Boot to iSCSI target	Controls whether the iSCSI boot host software attempts to boot from the iSCSI target after successfully connecting to it. When the option is enabled, the iSCSI boot host software immediately attempts to boot form the iSCSI target. If set to disabled, the iSCSI boot host software does not attempt to boot from the iSCSI target and control returns to the system BIOS so that the next boot device may be used. The One Time Disabled option is used when you want to do a remote install of the OS to an iSCSI target. As the option is named, it is set to disable on the first boot, then changes to enabled on subsequent reboots to indicate that iSCSI boots from the iSCSI target.
DHCP Vendor ID	Controls how the iSCSI boot host software interprets the Vendor Class ID field used during DHCP. If the Vendor Class ID field in the DHCP Offer packet matches the value in the field, the iSCSI boot host software looks into the DHCP Option 43 fields for the required iSCSI boot extensions. If DHCP is disabled, this value does not need to be set.
Link Up Delay Time	Controls how long the iSCSI boot host software waits, in seconds, after an Ethernet link is established before sending any data over the network. The valid values are 0 to 255. As an example, a user may need to set a value for this option if a network protocol, such as Spanning Tree, is enabled on the switch interface to the client system.

Table 1: Configuration Options

Option	Description
Use TCP Timestamp	Controls if the TCP Timestamp option is enabled or disabled.
Target as First HDD	Allows specifying that the iSCSI target drive will appear as the first hard drive in the system.
LUN Busy Retry Count	Controls the number of connection retries the iSCSI Boot initiator will attempt if the iSCSI target LUN is busy.
IP Version	This option specific to IPv6. Toggles between the IPv4 or IPv6 protocol. All IP settings will be lost when switching from one protocol version to another.

MBA Boot Protocol Configuration

To configure the boot protocol

1. Restart your system.
2. From the PXE banner, select **CTRL+S**. The MBA Configuration Menu appears (see Broadcom Boot Agent).
3. From the MBA Configuration Menu, use the **UP ARROW** or **DOWN ARROW** to move to the **Boot Protocol** option. Use the **LEFT ARROW** or **RIGHT ARROW** to change the **Boot Protocol** option to **iSCSI**.
4. Select **iSCSI Boot Configuration** from **Main Menu**.

NOTE: If iSCSI boot firmware is not programmed in the NetXtreme network adapter, selecting **iSCSI Boot Configuration** will not have any effect.

iSCSI Boot Configuration

- Static iSCSI Boot Configuration
- Dynamic iSCSI Boot Configuration

Static iSCSI Boot Configuration

In a static configuration, you must enter data for the system's IP address, the system's initiator IQN, and the target parameters obtained in Configuring the iSCSI Target. For information on configuration options, see Table 1.

To configure the iSCSI boot parameters using static configuration

1. From the **General Parameters Menu** screen, set the following:
   - **TCP/IP parameters via DHCP**: Disabled. (For IPv4.)
   - **IP Autoconfiguration**: Disabled. (For IPv6)
   - **iSCSI parameters via DHCP**: Disabled
   - **CHAP Authentication**: Disabled
   - **Boot to iSCSI target**: Disabled
   - **DHCP Vendor ID**: BRCM ISAN
   - **Link Up Delay Time**: 0
   - **Use TCP Timestamp**: Enabled
   - **Target as First HDD**: Disabled
   - **LUN Busy Retry Count**: 0
   - **IP Version**: IPv6. (For IPv6)
2. Select **ESC** to return to the **Main** menu.

3. From the **Main** menu, select **Initiator Parameters**.
4. From the **Initiator Parameters** screen, type values for the following:
   - IP Address (unspecified IPv4 and IPv6 addresses should be "0.0.0.0" and "::", respectively**)**
   - Subnet Mask Prefix
   - Default Gateway
   - Primary DNS
   - Secondary DNS
   - iSCSI Name (corresponds to the iSCSI initiator name to be used by the client system)

   NOTE: Carefully enter the IP address. There is no error-checking performed against the IP address to check for duplicates or incorrect segment/network assignment.
5. Select **ESC** to return to the **Main** menu.
6. From the **Main** menu, select **1st Target Parameters**.
7. From the **1st Target Parameters** screen, enable **Connect** to connect to the iSCSI target. Type values for the following using the values used when configuring the iSCSI target:
   - IP Address
   - TCP Port
   - Boot LUN
   - iSCSI Name
8. Select **ESC** to return to the **Main** menu.
9. A second iSCSI boot adapter can be configured for redundancy in the event the primary adapter fails to boot. To configure the secondary device parameters, select **Secondary Device Parameters** from the **Main** menu (see Configure Parameters for a Secondary Adapter). Otherwise, go to step 10.
10. Select **ESC** and select **Exit and Save Configuration**.
11. Select **F4** to save your MBA configuration.
12. If necessary, return to the iSCSI Boot Configuration Utility to configure a second iSCSI target.

Dynamic iSCSI Boot Configuration

In a dynamic configuration, you only need to specify that the system's IP address and target/initiator information are provided by a DHCP server (see IPv4 and IPv6 configurations in Configuring the DHCP Server to Support iSCSI Boot). For IPv4, with the exception of the initiator iSCSI name, any settings on the Initiator Parameters, 1st Target Parameters, or 2nd Target Parameters screens are ignored and do not need to be cleared. For IPv6, with the exception of the CHAP ID and Secret, any settings on the Initiator Parameters, 1st Target Parameters, or 2nd Target Parameters screens are ignored and do not need to be cleared. For information on configuration options, see Table 1.

NOTE: When using a DHCP server, the DNS server entries are overwritten by the values provided by the DHCP server. This occurs even if the locally provided values are valid and the DHCP server provides no DNS server information. When the DHCP server provides no DNS server information, both the primary and secondary DNS server values are set to 0.0.0.0. When the Windows OS takes over, the Microsoft iSCSI initiator retrieves the iSCSI Initiator parameters and configures the appropriate registries statically. It will overwrite whatever is configured. Since the DHCP daemon runs in the Windows environment as a user process, all TCP/IP parameters have to be statically configured before the stack comes up in the iSCSI Boot environment.

If DHCP Option 17 is used, the target information is provided by the DHCP server, and the initiator iSCSI name is retrieved from the value programmed from the Initiator Parameters screen. If no value was selected, then the controller defaults to the name:

```
iqn.1995-05.com.broadcom.<11.22.33.44.55.66>.iscsiboot
```

where the string `11.22.33.44.55.66` corresponds to the controller's MAC address.

If DHCP option 43 (IPv4 only) is used, then any settings on the Initiator Parameters, 1st Target Parameters, or 2nd Target Parameters screens are ignored and do not need to be cleared.

To configure the iSCSI boot parameters using dynamic configuration

1. From the **General Parameters Menu** screen, set the following:
   - **TCP/IP parameters via DHCP**: Enabled. (For IPv4.)
   - **IP Autoconfiguration**: Enabled. (For IPv6)
   - **iSCSI parameters via DHCP**: Enabled
   - **CHAP Authentication**: Disabled
   - **Boot to iSCSI target**: Disabled
   - **DHCP Vendor ID**: BRCM ISAN
   - **Link Up Delay Time**: 0
   - **Use TCP Timestamp**: Enabled
   - **Target as First HDD**: Disabled
   - **LUN Busy Retry Count**: 0
   - **IP Version**: IPv6. (For IPv6)
2. Select **ESC** to return to the **Main** menu.

   NOTE: Information on the **Initiator Parameters 1st Target Parameters**, and **2nd Target Parameters** screens are ignored and do not need to be cleared.

3. A second iSCSI boot adapter can be configured for redundancy in the event the primary adapter fails to boot. To configure the secondary device parameters, select **Secondary Device Parameters** from the **Main** menu (see Configure Parameters for a Secondary Adapter). Otherwise, go to step 4.
4. Select **Exit and Save Configurations**.

Configure Parameters for a Secondary Adapter

A second iSCSI boot adapter can be optionally configured for redundancy in the event the primary adapter fails to boot.

To configure the iSCSI boot parameters for a secondary adapter

1. From the **iSCSI Boot Main Menu** screen, select **Secondary Device Parameters**.
2. From the **Device List**, select the adapter that will be used as the secondary adapter.
3. From the **Secondary Device Parameters** screen, set the following:
   - **Use Independent Target Portal:** Enabled (or Disabled if MPIO mode is not required)
   - **Use Independent Target Name**: Enabled
   - **Configure Secondary Device**: Invoke
4. Configure the secondary adapter parameters.

NOTE: The IP addresses for the primary and secondary adapters must be in two different subnets.

5. Select **ESC** and select **Exit and Save Configuration**.
6. Select **F4** to save your MBA configuration.

Enabling CHAP Authentication

Ensure that CHAP authentication is enabled on the target.

To enable CHAP authentication

1. From the **General Parameters** screen, set **CHAP Authentication** to Enabled.
2. From the **Initiator Parameters** screen, type values for the following:
   - CHAP ID (up to 128 bytes)
   - CHAP Secret (if authentication is required, and must be 12 characters in length or longer)
3. Select **ESC** to return to the **Main** menu.
4. From the **Main** menu, select **1st Target Parameters**.
5. From the **1st Target Parameters** screen, type values for the following using the values used when configuring the iSCSI target:
   - CHAP ID (optional if two-way CHAP)
   - CHAP Secret (optional if two-way CHAP, and must be 12 characters in length or longer)
6. Select **ESC** to return to the **Main** menu.
7. Select **ESC** and select **Exit and Save Configuration**.

Configuring the DHCP Server to Support iSCSI Boot

The DHCP server is an optional component and it is only necessary if you will be doing a dynamic iSCSI Boot configuration setup (see Dynamic iSCSI Boot Configuration).

Configuring the DHCP server to support iSCSI boot is different for IPv4 and IPv6.

- DHCP iSCSI Boot Configurations for IPv4
- DHCP iSCSI Boot Configuration for IPv6

DHCP iSCSI Boot Configurations for IPv4

The DHCP protocol includes a number of options that provide configuration information to the DHCP client. For iSCSI boot, Broadcom adapters support the following DHCP configurations:

- DHCP Option 17, Root Path
- DHCP Option 43, Vendor-Specific Information

DHCP Option 17, Root Path

Option 17 is used to pass the iSCSI target information to the iSCSI client.

The format of the root path as defined in IETC RFC 4173 is:

```
"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"
```

The parameters are defined below.

Table 2: DHCP Option 17 Parameter Definition

Parameter	***Definition***
`"iscsi:"`	A literal string
`<servername>`	The IP address or FQDN of the iSCSI target
`":"`	Separator
`<protocol>`	The IP protocol used to access the iSCSI target. Currently, only TCP is supported so the protocol is 6.
`<port>`	The port number associated with the protocol. The standard port number for iSCSI is 3260.
`<LUN>`	The Logical Unit Number to use on the iSCSI target. The value of the LUN must be represented in hexadecimal format. A LUN with an ID OF 64 would have to be configured as 40 within the option 17 parameter on the DHCP server.
`<targetname>`	The target name in either IQN or EUI format (refer to RFC 3720 for details on both IQN and EUI formats). An example IQN name would be “iqn.1995-05.com.broadcom:iscsi-target”.

DHCP Option 43, Vendor-Specific Information

DHCP option 43 (vendor-specific information) provides more configuration options to the iSCSI client than DHCP option 17. In this configuration, three additional suboptions are provided that assign the initiator IQN to the iSCSI boot client along with two iSCSI target IQNs that can be used for booting. The format for the iSCSI target IQN is the same as that of DHCP option 17, while the iSCSI initiator IQN is simply the initiator's IQN.

NOTE: DHCP Option 43 is supported on IPv4 only.

The suboptions are listed below.

Table 3: DHCP Option 43 Suboption Definition

Suboption	***Definition***
201	First iSCSI target information in the standard root path format `"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"`
202	Second iSCSI target information in the standard root path format `"iscsi:"<servername>":"<protocol>":"<port>":"<LUN>":"<targetname>"`
203	iSCSI initiator IQN

Using DHCP option 43 requires more configuration than DHCP option 17, but it provides a richer environment and provides more configuration options. Broadcom recommends that customers use DHCP option 43 when performing dynamic iSCSI boot configuration.

Configuring the DHCP Server

Configure the DHCP server to support option 17 or option 43.

NOTE: If using Option 43, you also need to configure Option 60. The value of Option 60 should match the **DHCP**

Vendor ID value. The **DHCP Vendor ID** value is BRCM ISAN, as shown in **General Parameters** of the iSCSI Boot Configuration menu.

DHCP iSCSI Boot Configuration for IPv6

The DHCPv6 server can provide a number of options, including stateless or stateful IP configuration, as well s information to the DHCPv6 client. For iSCSI boot, Broadcom adapters support the following DHCP configurations:

- DHCPv6 Option 16, Vendor Class Option
- DHCPv6 Option 17, Vendor-Specific Information

NOTE: The DHCPv6 standard Root Path option is not yet available. Broadcom suggests using Option 16 or Option 17 for dynamic iSCSI Boot IPv6 support.

DHCPv6 Option 16, Vendor Class Option

DHCPv6 Option 16 (vendor class option) must be present and must contain a string that matches your configured **DHCP Vendor ID** parameter. The **DHCP Vendor ID** value is BRCM ISAN, as shown in **General Parameters** of the iSCSI Boot Configuration menu.

The content of Option 16 should be <2-byte length> <DHCP Vendor ID>.

DHCPv6 Option 17, Vendor-Specific Information

DHCPv6 Option 17 (vendor-specific information) provides more configuration options to the iSCSI client. In this configuration, three additional suboptions are provided that assign the initiator IQN to the iSCSI boot client along with two iSCSI target IQNs that can be used for booting.

The suboptions are listed below.

Table 4: DHCP Option 17 Suboption Definition

Suboption	***Definition***
201	First iSCSI target information in the standard root path format `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
202	Second iSCSI target information in the standard root path format `"iscsi:"[<servername>]":"<protocol>":"<port>":"<LUN>":"<targetname>"`
203	iSCSI initiator IQN

NOTE: In Table 4, the brackets [ ] are required for the IPv6 addresses.

The content of option 17 should be <2-byte Option Number 201|202|203> <2-byte length> <data>.

Configuring the DHCP Server

Configure the DHCP server to support Option 16 and Option 17.

NOTE: The format of DHCPv6 Option 16 and Option 17 are fully defined in RFC 3315.

Preparing the iSCSI Boot Image

- Windows Server 2008 R2 and SP2 iSCSI Boot Setup
- Windows Server 2012 iSCSI Boot Setup
- Linux iSCSI Boot Setup
- Injecting (Slipstreaming) the Broadcom Drivers into Windows Image Files

Windows Server 2008 R2 and SP2 iSCSI Boot Setup

Windows Server 2008 R2 and Windows Server 2008 SP2 support iSCSI booting. The following procedure references Windows Server 2008 R2 but is common to both the Windows Server 2008 R2 and SP2.

Required CD/ISO image:

- Windows Server 2008 R2 x64 with the Broadcom drivers injected. See Injecting (Slipstreaming) the Broadcom Drivers into Windows Image Files. Also refer to the Microsoft knowledge base topic KB974072 at support.microsoft.com.

Other software required:

- Bindview.exe (Windows Server 2008 R2 only; see KB976042)

Procedure:

1. Remove any local hard drives on the system to be booted (the “remote system”).
2. Load the latest Broadcom MBA and iSCSI boot images onto NVRAM of the adapter.
3. Configure the BIOS on the remote system to have the Broadcom MBA as the first bootable device, and the CDROM as the second device.
4. Configure the iSCSI target to allow a connection from the remote device. Ensure that the target has sufficient disk space to hold the new O/S installation.
5. Boot up the remote system. When the Preboot Execution Environment (PXE) banner displays, press **Ctrl+S** to enter the PXE menu.
6. At the PXE menu, set **Boot Protocol** to **iSCSI**.
7. Enter the iSCSI target parameters.
8. In General Parameters, set the **Boot to Target** parameter to **One-Time Disabled.**
9. Save the settings and reboot the system.

   The remote system should connect to the iSCSI target and then boot from the DVDROM device.
10. Boot to DVD and begin installation.
11. Answer all the installation questions appropriately (specify the Operating System you want to install, accept the license terms, etc.).

    When the **Where do you want to install Windows?** window appears, the target drive should be visible. This is a drive connected via the iSCSI boot protocol, located in the remote iSCSI target.
12. Select **Next** to proceed with Windows Server 2008 R2 installation.

    A few minutes after the Windows Server 2008 R2 DVD installation process starts, a system reboot will follow. After the reboot, the Windows Server 2008 R2 installation routine should resume and complete the installation.
13. Following another system restart, check and verify that the remote system is able to boot to the desktop.
14. After Windows Server 2008 R2 is booted up, load the driver and run Bindview.exe.
    a. Select **All Services**.
    b. Under **WFP Lightweight Filter** you should see **Binding paths** for the AUT. Right-click and disable them. When

done, close out of the application.

15. Verify that the OS and system are functional and can pass traffic by pinging a remote system's IP, etc.

Windows Server 2012 iSCSI Boot Setup

Windows Server 2012 supports iSCSI booting and installation. Broadcom requires the use of a “slipstream” DVD with the latest Broadcom drivers injected. See Injecting (Slipstreaming) the Broadcom Drivers into Windows Image Files. Also refer to the Microsoft knowledge base topic KB974072 at support.microsoft.com.

The following procedure prepares the image for installation and booting:

1. Remove any local hard drives on the system to be booted (the “remote system”).
2. Load the latest Broadcom MBA and iSCSI boot images into the NVRAM of the adapter.
3. Configure the BIOS on the remote system to have the Broadcom MBA as the first bootable device and the CDROM as the second device.
4. Configure the iSCSI target to allow a connection from the remote device. Ensure that the target has sufficient disk space to hold the new O/S installation.
5. Boot up the remote system. When the Preboot Execution Environment (PXE) banner displays, press **Ctrl+S** to enter the PXE menu.
6. At the PXE menu, set **Boot Protocol** to **iSCSI**.
7. Enter the iSCSI target parameters.
8. In General Parameters, set the **Boot to Target** parameter to **One-Time Disabled**.
9. Save the settings and reboot the system.

   The remote system should connect to the iSCSI target and then boot from the DVDROM device.
10. Boot from DVD and begin installation.
11. Answer all the installation questions appropriately (specify the Operating System you want to install, accept the license terms, etc.).

    When the **Where do you want to install Windows?** window appears, the target drive should be visible. This is a drive connected via the iSCSI boot protocol, located in the remote iSCSI target.
12. Select **Next** to proceed with Windows 2012 installation.

    A few minutes after the Windows 2012 DVD installation process starts, a system reboot will occur. After the reboot, the Windows 2012 installation routine should resume and complete the installation.
13. Following another system restart, check and verify that the remote system is able to boot to the desktop.
14. After Windows 2012 boots to the OS, Broadcom recommends running the driver installer to complete the Broadcom driver and application installation.

Linux iSCSI Boot Setup

Linux iSCSI boot is supported on Red Hat Enterprise Linux 5.5 and later and SUSE Linux Enterprise Server 10.x, 11, 11 SP1, and later.

There are two methods to set up Linux iSCSI boot:

- Local hard drive installation
- Remote DVD installation

Local hard drive installation

1. Install Linux OS on your local hard drive and make sure open-iscsi initiator is up to date.
2. Make sure all Runlevels of network service are on.
3. Make sure 2, 3, and 5 Runlevels of iscsi service are on.
4. Update uIP. You can get uIP package from Broadcom CD. This step is not needed for SuSE 10.
5. Install linux-nx2 package on you linux system. You can get this package from Broadcom CD.
6. Install bibt package on you Linux system. You can get this package from Broadcom CD.
7. Delete all ifcfg-eth* files.
8. Configure one port of network adapter to connect to iSCSI Target (see how to setup iSCSI target in corresponding section).
9. Connect to iSCSI Target.
10. Use DD command to copy local hard drive to iSCSI Target.
11. When DD is done, execute sync command a couple of times, logout then login to iSCSI Target again.
12. Run fsck command on all partitions created on iSCSI Target.
13. Change to /OPT/bcm/bibt folder and run the iscsi_setup.sh script to create the initrd images. Choose Option 0 to create the appropriate image type for iSCSI boot.
14. Mount the /boot partition on the iSCSI Target.
15. Copy the initrd images you created in step 13 from your local hard drive to the partition mounted in step 14.
16. On the partition mounted in step 14, edit grub menu to point to the new initrd images.
17. Unmount the /boot partition on the iSCSI Target.
18. (Red hat Only) To enable CHAP, you need to modify the CHAP section of the iscsid.conf file on the iSCSI Target. Edit iscsid.conf file with one or two way CHAP information as desired.
19. Shut down system and disconnect local hard drive. Now you are ready to iSCSI boot into iSCSI Target.
20. Configure iSCSI Boot Parameters including CHAP parameters if desired (see corresponding sections).
21. Continue booting into iSCSI Boot image and choose the image you created.

Remote DVD installation

After completing the installation, the system can be set up for iSCSI boot as described in the procedure below.

1. Get the latest Broadcom Linux driver CD.
2. Configure iSCSI Boot Parameters for DVD direct install to target by disabling Boot from target option on network adapter.
3. Change boot order as follows:
   a. Boot from the network adapter.
   b. Boot from the CD/DVD driver.
4. Reboot the system.
5. System will connect to iSCSI target, then will boot from CD/DVD drive.
6. Follow the corresponding OS instructions.
   a. Red Hat 5.5 - Type “linux dd” at “boot:” prompt and press enter
   b. Red Hat 6.0
   c. SuSE 10
   d. SuSE 11.1 choose “installation” and type withiscsi=1 netsetup=1 at boot option and choose YES for F6 driver option.
7. Follow the instructions to load the driver CD.

8. At the “networking device” prompt, choose the desired network adapter port and press **OK**.
9. At “configure TCP/IP prompt”, configure the way the system acquire IP address and press **OK**.
10. If static IP was chosen, you need to enter IP information for iscsi initiator.
11. (Red hat) choose to “skip” media testing.
12. Continue installation as desired. A drive will be available at this point. After file copying is done, remove CD/DVD and reboot system.
13. When system reboot, enable “boot from target” in iSCSI Boot Parameters and continue with installation until it is done.
14. Update iscsi initiator if needed. You need to remove existing one first.
15. Make sure all runlevels of network service are on.
16. Make sure 2,3 and 5 runlevels of iscsi service are on.
17. For Red Hat 6.0, make sure Network Manager service is stopped and disabled.
18. Install uIP (not required for SuSE 10).
19. Install linux-nx2 package.
20. Install bibt package.
21. Remove ifcfg-eth*.
22. Reboot.
23. For SUSE 11.1, follow remote DVD installation workaround.
24. After system reboot, login and change to /opt/bcm/bibt folder and run iscsi_setup.sh script to create the initrd image.
25. Copy the initrd images, to the /boot folder.
26. Change the grub menu to point to the new initrd image.
27. To enable CHAP you need to modify iscsid.conf (Red Hat only).
28. Reboot and change CHAP parameters if desired.
29. Continue booting into the iSCSI Boot image and select the image you created.

SUSE 11.1 Remote DVD installation workaround

1. Create a new file called boot.open-iscsi with the content shown below.
2. Copy the file you just created to /etc/init.d/ folder and overwrite the existing one.

Content of the new boot.open-iscsi file:

```
#!/bin/bash
#
# /etc/init.d/iscsi
#
### BEGIN INIT INFO
# Provides:          iscsiboot
# Required-Start:
# Should-Start:      boot.multipath
# Required-Stop:
# Should-Stop:       $null
# Default-Start:     B
# Default-Stop:
# Short-Description: iSCSI initiator daemon root-fs support
# Description:       Starts the iSCSI initiator daemon if the
#                    root-filesystem is on an iSCSI device
#
```

```
### END INIT INFO

ISCSIADM=/sbin/iscsiadm
ISCSIUIO=/sbin/iscsiuio
CONFIG_FILE=/etc/iscsid.conf
DAEMON=/sbin/iscsid
ARGS="-c $CONFIG_FILE"

# Source LSB init functions
. /etc/rc.status

#
# This service is run right after booting. So all targets activated
# during mkinitrd run should not be removed when the open-iscsi
# service is stopped.
#
iscsi_load_iscsiuio()
{
    TRANSPORT=`$ISCSIADM -m session 2> /dev/null | grep "bnx2i"`
    if [ "$TRANSPORT" ] ; then
   echo -n "Launch iscsiuio "
        startproc $ISCSIUIO
    fi
}

iscsi_mark_root_nodes()
{
    $ISCSIADM -m session 2> /dev/null | while read t num i target ; do
   ip=${i%%:*}
   STARTUP=`$ISCSIADM -m node -p $ip -T $target 2> /dev/null | grep "node.conn\[0\].startup"
| cut -d' ' -f3`
   if [ "$STARTUP" -a "$STARTUP" != "onboot" ] ; then
       $ISCSIADM -m node -p $ip -T $target -o update -n node.conn[0].startup -v onboot
   fi
    done
}

# Reset status of this service
rc_reset

# We only need to start this for root on iSCSI
if ! grep -q iscsi_tcp /proc/modules ; then
    if ! grep -q bnx2i /proc/modules ; then
        rc_failed 6
        rc_exit
    fi
fi

case "$1" in
    start)
   echo -n "Starting iSCSI initiator for the root device: "
   iscsi_load_iscsiuio
   startproc $DAEMON $ARGS
   rc_status -v
   iscsi_mark_root_nodes
   ;;
```

```
     stop|restart|reload)
    rc_failed 0
    ;;
     status)
    echo -n "Checking for iSCSI initiator service: "
    if checkproc $DAEMON ; then
        rc_status -v
    else
        rc_failed 3
        rc_status -v
    fi
    ;;
     *)
    echo "Usage: $0 {start|stop|status|restart|reload}"
    exit 1
    ;;
esac
rc_exit
```

Injecting (Slipstreaming) the Broadcom Drivers into Windows Image Files

To inject the Broadcom drivers into the Windows image files, you must obtain the correct Broadcom driver package for the applicable Windows Server version (2008 R2, 2008 SP2, or 2012). The package is named b57nd60a.

Then, you place the driver package to a working directory. For example, copy the driver package to the following directory:

- C:\Temp\b57nd60a

Finally, you inject the driver into the Windows Image (WIM) files and install the applicable Windows Server version from the updated images.

The detailed steps are provided below:

NOTE: The file and folder names used in this procedure are examples only. You can specify your own file and folder names for your slipstream project.

1. For Windows Server 2008 R2 and SP2, install the Windows Automated Installation Kit (AIK).
   —or—
   For Windows Server 2012, install the Windows Assessment and Deployment Kit (ADK).
2. Use the following commands to create a temporary directory and set it as the current directory for all later steps:
   ```
   md C:\Temp\x
   cd /d C:\Temp\x
   ```
3. Use the following commands to create two subdirectories:
   ```
   md src
   md mnt
   ```
4. Use the following command to copy the original DVD into the src subdirectory.
   ```
   xcopy N:\ .\src /e /c /i /f /h /k /y /q
   ```
   Note that in this example, the installation DVD is in the N: drive.
5. Open a Deployment and Imaging Tools command prompt in elevated mode. Then, set c:\Temp\x as the current directory.

   Note that you will use this command prompt window in all subsequent steps.

6. Enter the following commands:
   ```
   attrib -r .\src\sources\boot.wim
   attrib -r .\src\sources\install.wim
   ```
7. Enter run the following command to mount the boot.wim image:
   ```
   dism /mount-wim /wimfile:.\src\sources\boot.wim /index:2 /mountdir:.\mnt
   ```
   Note that you must always use “2” for the index value.
8. Enter the following commands to add the following driver to the currently mounted image:
   ```
   dism /image:.\mnt /add-driver /driver:C:\Temp\b57nd60a\b57nd60a.inf
   ```
9. Enter the following command to unmount the boot.wim image:
   ```
   dism /unmount-wim /mountdir:.\mnt /commit
   ```
10. Enter the following command to determine the index of the desired SKU in the install.wim image:
    ```
    dism /get-wiminfo /wimfile:.\src\sources\install.wim
    ```
    For example, in Windows Server 2012, index 2 is identified as “Windows Server 2012 SERVERSTANDARD.”
11. Enter the following command to mount the install.wim image:
    ```
    dism /mount-wim /wimfile:.\src\sources\install.wim /index:X /mountdir:.\mnt
    ```
    Note that X is a placeholder for the index value that you obtained in step 10.
12. Enter the following commands to add the driver to the currently mounted image:
    ```
    dism /image:.\mnt /add-driver /driver:C:\Temp\b57nd60a\b57nd60a.inf
    ```
13. Enter the following command to unmount the install.wim image:
    ```
    dism /unmount-wim /mountdir:.\mnt /commit
    ```
14. Enter the following command to create an .iso file:
    ```
    oscdimg -e -h -m -n -lslipstream -bootdata:2#p0,e,b"c:\Program Files\Windows
    AIK\Tools\PETools\amd64\boot\etfsboot.com"#pEF,e,b"c:\Program Files\Windows
    AIK\Tools\PETools\amd64\boot\efisys.bin" c:\temp\x\src c:\temp\Win20xxMOD.iso
    ```
    Note that Platform is a placeholder for the architecture of the operating system that you want to install, such as amd64 or x86. Also, xx in the file names is a placeholder for the Windows Server OS version (2012, 2008R2, 2008SP2.)
15. Using a DVD-burning application, burn the .iso file you created to a DVD.
16. Use the DVD that you created in step 15 to install the applicable Windows Server version.

Booting

After that the system has been prepared for an iSCSI boot and the operating system is present on the iSCSI target, the last step is to perform the actual boot. The system will boot to Windows or Linux over the network and operate as if it were a local disk drive.

1. Reboot the server.
2. Select **CTRL+S**.
3. From the **Main** menu, select **General Parameters** and configure the **Boot to iSCSI target** option to **Enabled**.

If CHAP authentication is needed, enable CHAP authentication after determining that booting is successful (see Enabling CHAP Authentication).

Other iSCSI Boot Considerations

There are several other factors that should be considered when configuring a system for iSCSI boot.

Changing the Speed & Duplex Settings in Windows Environments

Booting via the NDIS path is supported. The Speed & Duplex settings can be changed using the BACS management utility for iSCSI boot via the NDIS path.

Virtual LANs

Virtual LAN (VLAN) tagging is not supported for iSCSI boot with the Microsoft iSCSI Software Initiator.

TROUBLESHOOTING ISCSI BOOT

The following troubleshooting tips are useful for iSCSI boot.

Problem: A system blue screen occurs when iSCSI boots Windows Server 2008 R2 through the adapter's NDIS path with the initiator configured using a link-local IPv6 address and the target configured using a router-configured IPv6 address.
Solution: This is a known Windows TCP/IP stack issue.

Problem: The Broadcom iSCSI Crash Dump utility will not work properly to capture a memory dump when the link speed for iSCSI boot is configured for 10 Mbps or 100 Mbps.
Solution: The iSCSI Crash Dump utility is supported when the link speed for iSCSI boot is configured for 1 Gbps or 10 Gbps. 10 Mbps or 100 Mbps is not supported.

Problem: An iSCSI target is not recognized as an installation target when you try to install Windows Server 2008 by using an IPv6 connection.
Solution: This is a known third-party issue. See Microsoft Knowledge Base KB 971443, http://support.microsoft.com/kb/971443.

Problem: The iSCSI configuration utility will not run.
Solution: Ensure that the iSCSI Boot firmware is installed in the NVRAM.

Problem: A system blue screen occurs when installing the Broadcom drivers through Windows Plug-and-Play (PnP).
Solution: Install the drivers through the Setup installer.

Problem: After configuring the iSCSI boot LUN to 255, a system blue screen appears when performing iSCSI boot.
Solution: Although Broadcom's iSCSI solution supports a LUN range from 0 to 255, the Microsoft iSCSI software initiator does not support a LUN of 255. Configure a LUN value from 0 to 254.

Problem: NDIS miniports with Code 31 yellow-bang after L2 iSCSI boot install.
Solution: Run the T7.4 installer.

Problem: Unable to update inbox driver if a non-inbox hardware ID present.
Solution: Create a custom slipstream DVD image with supported drivers present on the install media.

Problem: Installing Windows onto an iSCSI target via iSCSI boot fails when connecting to a 1 Gbps switch port.
Solution: This is a limitation relating to adapters that use SFP+ as the physical connection. SFP+ defaults to 10 Gbps operation and does not support autonegotiation.

iSCSI Crash Dump

If you will use the Broadcom iSCSI Crash Dump utility, it is important to follow the installation procedure to install the iSCSI Crash Dump driver. See Using the Installer for more information.

NDIS2 Driver Software: Broadcom NetXtreme 57XX User Guide

Preinstallation Requirements

Before you can successfully install the NDIS2 driver software, the Broadcom network adapter must be physically installed in the server. Networking software that is appropriate to the operating system (such as Microsoft LAN Manager 2.2 for MS-DOS) must already be running on your server.

Installing the NDIS2 Driver Software for Use on MS-DOS Platforms

The NDIS2 driver software can be run from an MS-DOS startup disk using Microsoft Network Client 3.0 or from the hard disk using Microsoft LAN Manager 2.2.

Creating a Startup Disk to Run Microsoft Network Client

To perform this installation you must have the following items:

- Windows NT Server 4.0 CD-ROM
- A blank MS-DOS system disk (3.5" high-density floppy disk)
- Access to the Broadcom NDIS2 driver file (B57.dos). This file is located on the installation CD.

NOTES:

- **Windows NT Server 4.0 users.** When running **Setup for Microsoft Network Client v3.0 for MS-DOS**, click any network card from the list (**NE2000 Compatible**, for example) to create the startup disk.
- After creating the startup disk, follow the instructions in Modifying the Startup Disk.

To create a startup disk

1. Create a folder called NCADMIN in the root of the C drive.
2. Copy the NCADMIN.CN_, NCADMIN.EX_, and NCADMIN.HL_ files from the I386 folder on the Windows NT Server 4.0 CD-ROM.

3. Open a command prompt window and change the directory to C:\NCADMIN.
4. Type **expand -r ncadmin.*** and press ENTER.
5. Close the command prompt window by typing exit and then pressing **ENTER**.
6. Start Windows Explorer.
7. Open the NCADMIN folder and double-click **ncadmin.exe**.
8. Follow the on-screen instructions to make the network startup disk (choose **NE2000 Compatible** from the list of adapters).

MODIFYING THE STARTUP DISK

To modify the startup disk

1. Edit A:\Net\Protocol.ini with Notepad or a similar text editor.
   a. Change DriverName=$ to DriverName=B57$.
   b. Remove all other parameter entries under the [MS$NE2CLONE] or equivalent section such as IOBASE=0x300 or INTERRUPT=3, and so on.

   Example Protocol.ini file for IP

```
[network.setup]
version=0x3110
netcard=ms$ne2clone,1,MS$NE2CLONE,1
transport=tcpip,TCPIP
lana0=ms$ne2clone,1,tcpip
[MS$NE2CLONE]
DriverName=B57$
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
[tcpip]
NBSessions=6
DefaultGateway=0
SubNetMask=255 0 0 0
IPAddress=192 168 0 1
DisableDHCP=0
DriverName=TCPIP$
BINDINGS=MS$NE2CLONE
LANABASE=0
```

   Example: Protocol.ini file for IPX

```
[network.setup]
version=0x3110
netcard=ms$ne2clone,1,MS$NE2CLONE,1
transport=ms$ndishlp,MS$NDISHLP
transport=ms$nwlink,MS$NWLINK
lana0=ms$ne2clone,1,ms$nwlink
lana1=ms$ne2clone,1,ms$ndishlp
[MS$NE2CLONE]
DriverName=B57$
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
[MS$NDISHLP]
DriverName=ndishlp$
```

```
BINDINGS=ms$ne2clone
[ms$nwlink]
DriverName=nwlink$
FRAME=Ethernet_802.2
BINDINGS=MS$NE2CLONE
LANABASE=0
```

Example Protocol.ini file for NetBEUI

```
[network.setup]
version=0x3110
netcard=ms$ne2clone,1,MS$NE2CLONE,1
transport=ms$ndishlp,MS$NDISHLP
transport=ms$netbeui,MS$NETBEUI
lana0=ms$ne2clone,1,ms$ndishlp
lana1=ms$ne2clone,1,ms$netbeui
[MS$NE2CLONE]
DriverName=B57$
[protman]
DriverName=PROTMAN$
PRIORITY=MS$NDISHLP
[MS$NDISHLP]
DriverName=ndishlp$
BINDINGS=MS$NE2CLONE
[MS$NETBEUI]
DriverName=netbeui$
SESSIONS=10
NCBS=12
BINDINGS=MS$NE2CLONE
LANABASE=0
```

2. Edit A:\Net\System.ini.
   a. Change netcard= to netcard=b57.dos.
   b. Check for references to C:\NET and change C:\NET to A:\NET if necessary.

Example System.ini file

```
[network]
sizworkbuf=1498
filesharing=no
printsharing=no
autologon=yes
computername=MYPC
lanroot=A:\NET
username=USER1
workgroup=WORKGROUP
reconnect=yes
dospophotkey=N
lmlogon=0
logondomain=
preferredredir=basic
autostart=basic
maxconnections=8
[network drivers]
netcard=B57.dos
transport=ndishlp.sys,*netbeui
```

```
devdir=A:\NET
LoadRMDrivers=yes
```

3. Copy B57.dos to A:\Net.
4. Create the appropriate Autoexec.bat file in drive A for the chosen protocol as shown below.

   For TCP/IP

   ```
   path=a:\net
   a:\net\net initialize
   a:\net\netbind.com
   a:\net\umb.com
   a:\net\tcptsr.exe
   a:\net\tinyrfc.exe
   a:\net\nmtsr.exe
   a:\net\emsbfr.exe
   a:\net\net start basic
   net use z: \\SERVERNAME\SHARENAME
   ```

   For IPX

   ```
   SET PATH=A:\NET
   A:\NET\net initialize
   A:\NET\nwlink
   A:\NET\NET START BASIC
   net use z: \\SERVERNAME\SHARENAME
   ```

   For NetBEUI

   ```
   SET PATH=A:\NET
   A:\NET\NET START BASIC
   net use z: \\SERVERNAME\SHARENAME
   ```

5. Create a Config.sys file on the startup disk in drive A as shown below.

   ```
   files=30
   device=a:\net\ifshlp.sys
   lastdrive=z
   ```

INSTALLING THE DOS NDIS2 DRIVER SOFTWARE ON THE HARD DISK

To install the DOS NDIS2 Driver Software on the hard disk

1. Verify that the system has Microsoft LAN Manager 2.2 installed, with a protocol such as NetBEUI configured.
2. Create a folder on your hard disk to store the NDIS 2.01 driver.
   Example: C:\LANMAN
3. Copy the B57.dos file to this folder.
4. Edit the Config.sys file by adding the following lines:

   ```
   DEVICE = C:\LANMAN\PROTMAN.DOS
   DEVICE = C:\LANMAN\B57.DOS
   DEVICE = C:\LANMAN\NETBEUI.DOS
   ```

5. Edit the Autoexec.bat file by adding the following lines:

   ```
   C:\LANMAN\NETBIND.EXE
   C:\LANMAN\NET START WORKSTATION
   C:\LANMAN\NET USE drive letter: \\server name\resource name
   ```

6. Edit the Protocol.ini file (located in C:\LANMAN) to configure the driver to bind with NetBEUI or any other protocols.
   Example:

   ```
   [PROTOCOL MANAGER]
   ```

```
DriverName = PROTMAN$
[NETBEUI_XIF]
DriverName = netbeui$
BINDINGS = B57
[B57]
DriverName = "B57$"
```

7. Restart the computer to complete the installation.

NOTE: The driver loads during system configuration and displays the Broadcom banner, controller name, MAC address, IRQ number, detected line speed, and the controller BusNum and DevNum. If the driver fails to load, an *initialization fail* message is displayed.

CONFIGURING THE NDIS2 DRIVER SOFTWARE

The NDIS2 driver software can be configured by adding specific optional keywords to the Protocol.ini file. If multiple (or multiport) Broadcom NetXtreme Gigabit Ethernet adapters are installed in a system, the NDIS2 driver software loads by default on the adapter/port that has a good link. If 2 or more adapters have a good link, the NDIS2 driver software loads on the adapter having the latest Device ID. If 2 or more adapters that have a good link have the same Device ID, the NDIS2 driver software loads on the adapter that is located in the slot having the lowest bus number.

NOTE: On MS-DOS platforms, it is not recommended to load the NDIS2 driver software on more than 1 adapter; the required NDIS2 protocol manager that supports multiple binds is not available in the MS-DOS environment.

If it is necessary to have the NDIS2 driver load on certain adapters in a certain order, the BusNum, DevNum, and FuncNum keywords can be used. Do not use these keywords unless you know how to configure PCI devices.

The **BusNum** keyword value, which represents the PCI bus number in which the adapter is located, is a decimal number ranging from 0 to 255.

The **FuncNum** keyword value, which represents the function (port) number of a multiport adapter, is a decimal number, with 0 representing the first port, and 1 representing the second port.

The **DevNum** keyword value, which represents the assigned device number, is a decimal number ranging from 0 to 31.

NOTE: At the end of the NDIS2 driver software installation process, note the BusNum and DevNum values that are displayed. Alternatively, use Broadcom Advanced Control Suite (see Broadcom Advanced Control Suite) to view the bus number, function (port) number, and device number assigned to each adapter (Windows users only).

Example BusNum, DevNum, and FuncNum keyword entries for loading the NDIS2 driver on multiple adapters in a certain order are shown below:

```
[B57]
DRIVERNAME = B57$
BUSNUM = 3
DEVNUM = 10
[B57_2]
```

```
DRIVERNAME = B572$
BUSNUM 3
DEVNUM 11
[B57_3]
DRIVERNAME = B573$
BUSNUM 3
DEVNUM 12
[B57_4]
DRIVERNAME = B574$
BUSNUM 3
DEVNUM 13
```

The LineSpeed keyword is used to force the speed of the network connection. The LineSpeed keyword requires a decimal number and of either 10, 100, or 1000. Technically, a line speed of 1000 Mbit/s cannot be forced and can be achieved only through auto-negotiation. For the sake of simplicity, the driver performs auto-negotiation when the line speed is set to a value of 1000. Forced 1000 Mbit/s speed is not needed for copper links; auto-negotiation is the proper supported configuration under the IEEE Ethernet specification.

The Duplex keyword is used to force the duplex mode of the adapter. The Duplex keyword requires a text string of either HALF or FULL. When the Duplex keyword is used, the LineSpeed keyword must also be used. If neither keyword is used, the network adapter defaults to auto-negotiation mode.

The NodeAddress keyword specifies the network address used by the adapter. If a multicast address or a broadcast address is specified, the adapter uses the default MAC address.

The FixCheckSumOff keyword turns off the driver workaround for the TCP/IP stack to recognize the ones complement version of the checksum.

Example entries for the LineSpeed, Duplex, and NodeAddress keywords are shown below:

```
[B57]
DRIVERNAME = B57$
BUSNUM = 3
DEVNUM = 10
PORTNUM = 0
LINESPEED = 100
DUPLEX = FULL
NODEADDRESS = “001020304050”
```

USING KEYWORDS FOR THE B57.DOS DRIVERS

The Protocol.ini file contains certain keywords that are used by the B57.dos drivers. These keywords are listed below:

BusNum. Specifies the number of the PCI bus on which the network adapter is located. Requires a decimal number having a value ranging from 0 to 255.

DevNum. Specifies the device number assigned to the network adapter when it is configured by the PCI BIOS. Requires a decimal number having a value ranging from 0 to 255.

FuncNum or PortNum. Specifies the PCI function or port number assigned to the network controller. Requires a decimal number having a value ranging from 0 to 7.

NOTE: These keywords, **BusNum**, **DevNum**, and **FuncNum** (or **PortNum**), are needed when multiple adapters are installed in the server and when a specific controller must be loaded in a certain order. These keywords are used concurrently and are included for manufacturing purposes. Do not use them unless you are familiar with how to configure PCI devices. A PCI device scan utility is needed to find this information.

LineSpeed. Specifies the speed of the network connection in Mbit/s. Requires the decimal number **10**, **100**, or **1000**. Technically, a line speed of 1000 Mbit/s cannot be forced and is achievable only through auto-negotiation. For the sake of simplicity, the driver performs auto-negotiation when the line speed is set to a value of 1000.

Duplex. Specifies the duplex mode of the network adapter. Requires a setting of either **Half** or **Full**. When this keyword is used, the **LineSpeed** keyword must also be used. If neither keyword is used, the network adapter defaults to auto-negotiation mode.

NodeAddress. Specifies the network address used by the network adapter. If a multicast address or a broadcast address is specified, the adapter uses the default MAC address.

Example:

```
[B57]
DriverName = "B57$"
BusNum = 3
DevNum = 14
PortNum = 2
LineSpeed = 1000
Duplex = Full
NodeAddress = 001020304050
```

Linux Driver Software: Broadcom NetXtreme 57XX User Guide

LIMITATIONS

The current version of the adapter driver has been tested on the latest Red Hat, SuSE, and other Linux distributions for i386, ia64, and x86_64 CPU architectures using 2.4.x and 2.6.x kernels. The driver has been tested up to kernel version 2.4.33 and 2.6.13. The driver should work on other little endian or big endian CPU architectures, but only very limited testing has been done on some of these machines. The Makefile may have to be modified to include architecture-specific compile switches, and some minor changes in the source files may also be required. On these machines, patching the driver into the kernel is recommended.

PACKAGING

The Linux TG3 driver is released in the following packaging formats (file names):

- Source RPM (tg3-*version*.src.rpm)
- Supplemental (tg3_sup-*version*.tar.gz)
- Compressed tar (tg3-*version*.tar.gz)

Identical source files to build the driver are included in both RPM and TAR source packages. The tar file contains additional utilities such as patches and driver disk images for network installation.

INSTALLING TG3 DRIVER SOFTWARE

- Installing the Source RPM Package
- Building the Driver from the Source TAR File

INSTALLING THE SOURCE RPM PACKAGE

Prerequisites:

- Linux kernel source
- C compiler

Procedure:

1. Install the source RPM package.
   ```
   rpm -ivh tg3-version.src.rpm
   ```
2. Change the directory to the RPM path and build the binary driver for your kernel (the RPM path is different for different Linux distributions).
   ```
   cd /usr/src/redhat,OpenLinux,turbo,packages,rpm …
   rpm -bb SPECS/tg3.spec or rpmbuild -bb SPECS/tg3.spec
   rpmbuild -bb SPECS/tg3.spec (for RPM version 4.x.x)
   ```

   NOTE: During your attempt to install a source RPM package, the following message may be displayed:

   ```
   error: cannot create %sourcedir /usr/src/redhat/SOURCE
   ```

   The most likely cause of the error is that the rpm-build package has not been installed. Locate the rpm-build package on the Linux installation media and install it using the following command:

   ```
   rpm -ivh rpm-build-version.i386.rpm
   ```

   Complete the installation of the source RPM.
3. Install the newly-built package (driver and man page).
   ```
   rpm -ivh RPMS/i386/tg3-version.i386.rpm
   ```
   Depending on the kernel, the driver is installed to one of the following paths:

   2.4.x kernels:

   /lib/modules/*kernel_version*/kernel/drivers/net/tg3.o

   2.4.x kernels with the tg3 driver patched in:

   /lib/modules/*kernel_version*/kernel/drivers/addon/tg3/tg3.o

   2.6.x kernels:

   /lib/modules/*kernel_version*/kernel/drivers/net/tg3.ko
4. Load the driver.
   ```
   modprobe tg3
   ```

To configure the network protocol and address, refer to the Linux version-specific documentation.

Building the Driver from the Source TAR File

1. Create a directory (tg3-*version*) and extract the TAR files to the directory.
   ```
   tar xvzf tg3-version.tgz
   ```
2. Build the driver tg3.o as a loadable module for the running kernel.
   ```
   CD tg3-version
   make clean
   make; make install
   ```
3. Test the driver by loading it.
   ```
   rmmod tg3
   modprobe tg3
   ```
   No message should be returned if this command runs properly.

   NOTE: See the RPM instructions above for the location of the installed driver.
4. To configure network protocol and address, refer to the manuals supplied with your operating system.

Network Installations

For network installations through NFS, FTP, or HTTP (using a network boot disk or PXE), a driver disk that contains the tg3 driver may be needed. The driver disk images for the most recent Red Hat versions are included. Boot drivers for other Linux versions can be compiled by modifying the Makefile and the make environment. Further information is available from the Red Hat website, http://www.redhat.com.

To create the driver disk, select the appropriate image file (located in tg3_sup-*version*.tar.gz) and type the following:

```
   dd if=<version>.dd.img of=/dev/fd0
```

Patching PCI Files (Optional)

For hardware detection utilities such as Red Hat kudzu to properly identify tg3 supported devices, a number of files containing PCI vendor and device information may need to be updated.

Apply the updates by running the scripts provided in the Supplemental tar file. For example, on Red Hat Enterprise Linux, apply the updates by doing the following:

```
./patch_pcitbl.sh  /usr/share/hwdata/pcitable pci.updates /usr/share/hwdata/pcitable.new

./patch_pciids.sh /usr/share/hwdata/pci.ids pci.updates /usr/share/hwdata/pci.ids.new
```

Next, the old files can be backed up and the new files can be renamed for use.

```
cp /usr/share/hwdata/pci.ids /usr/share/hwdata/old.pci.ids
cp /usr/share/hwdata/pci.ids.new /usr/share/hwdata/pci.ids

cp /usr/share/hwdata/pcitable /usr/share/hwdata/old.pcitable
```

```
cp /usr/share/hwdata/pcitable.new /usr/share/hwdata/pcitable
```

NOTE: The paths above are for Red Hat distributions. These paths may be different on other distributions.

Unloading/Removing the TG3 Driver

- Unloading/Removing the Driver from an RPM Installation
- Removing the Driver from a TAR Installation

Unloading/Removing the Driver from an RPM Installation

To unload the driver, use **ifconfig** to bring down all *ethX* interfaces opened by the driver, and then type the following:

```
rmmod tg3
```

If the driver was installed using **rpm**, do the following to remove it:

```
rpm -e tg3-<version>
```

Removing the Driver from a TAR Installation

If the driver was installed using make install from the tar file, the tg3.o driver file has to be manually deleted from the operating system. See Installing the Source RPM Package for the location of the installed driver.

If there is an interface configuration that is related to the tg3 driver, then bring the interface down first by using **ifconfig ethx down** and then **rmod tg3**.

DRIVER MESSAGES

The following are the most common sample messages that may be logged in the */var/log/messages* file. Use **dmesg -n*level*** to control the level at which messages appear on the console. Most systems are set to level 6 by default.

Driver Sign on

```
tg3.c:version (date)
```

NIC Detected

```
eth#: Tigon3 [partno (BCM95xxx) rev 4202 PHY (57xx) (PCI Express) 10/100/1000BaseT
Ethernet :00:xx:xx:xx:xx:xx
eth#: RXcsums [1] LinkChg REG [0] MIirq [0] ASF [0] Split [0] Wirespeed [1]TSOcap [1]
eth#: dma_rwctrl [76180000]
ACPI : PCI interrupt 0000:02:02.0 [A] -> GSI 26 (level,low) -> IRQ 233
```

Flow Control

```
tg3: eth#: Flow control is configured for TX and for RX.
```

Link Up and Speed Indication

```
tg3: eth#: Link is up at 1000 Mbps, full duplex.
```

Link Down Indication

```
tg3: eth#: Link is down.
```

TEAMING WITH CHANNEL BONDING

With the TG3 driver, you can team adapters together using the bonding kernel module and a channel bonding interface. Refer to your Red Hat documentation for more information on Linux Channel Bonding.

UNIX Driver Software: Broadcom NetXtreme® 57XX User Guide

NOTE: Before you proceed, review the Readme.txt file to see if there are any problems or limitations associated with the specific UNIX driver software you are using.

SCO UnixWare 7/Caldera Open UNIX 8 Driver

Driver Software Package

The driver is released as an installable package in datastream format.

Installing the Driver

1. Install the bcme package on the UnixWare system by typing the following:
```
pkgadd -d <install_path>
```
   where <install_path> is the path to the installable package (bcme-<version>.pkg)
2. After you have installed the package, carry out **netcfg** or **scoadmin network** to add the new network adapter.
3. When you are prompted, specify the settings for the Line Speed, Flow Control, and MAC Address properties. These properties (along with other properties) and the respective available settings are listed in Table 1.

Table 1: Advanced Properties

Property	*Setting*	*Comments*
Line Speed	Auto Negotiation (default)	All speeds advertised
	10 Mbps half-duplex fixed	
	10 Mbps half-duplex auto	Only 10 Mbps speed, half-duplex mode advertised
	10 Mbps full-duplex fixed	
	10 Mbps full-duplex auto	Only 10 Mbps speed, full-duplex mode advertised

Table 1: Advanced Properties (Cont.)

Property	Setting	Comments
	100 Mbps half-duplex fixed	
	100 Mbps half-duplex auto	Only 100 Mbps speed, half-duplex mode advertised
	100 Mbps full-duplex fixed	
	100 Mbps full-duplex auto	Only 100 Mbps speed, full-duplex mode advertised
	1000 Mbps full-duplex fixed[1]	
	1000 Mbps full-duplex auto	Only 1000 Mbps speed, full-duplex mode advertised
Flow Control	Auto Negotiation[2] (default) Disabled Receive Pause Transmit Pause Receive & Transmit Pause	Symmetric Pause advertised
MAC Address	No Override (default). A user-administered MAC address entered with a colon separating each hexadecimal byte, for example, 12:34:56:78:9A:BC	
Jumbo MTU Size	1500–9000 (default value is 1500)	
Wirespeed	Enabled[3] Disabled (default)	

[1] 1000 Mbps (1Gbps) full-duplex fixed speed is only valid for fiber connections. For copper twisted pair connections, 1 Gbps can only be set through auto negotiation with a 1 Gbps link partner.

[2] Auto negotiation of flow control is only valid when the line speed is set to auto negotiation (all speeds or single speed advertisements).

[3] Ethernet@Wirespeed™ allows the hardware to attempt to work with broken Ethernet cables. It is not recommended that this option be used when configuring interfaces in team.

After you have specified the settings for these properties, specify the network protocol and address when prompted.

Advanced Tunable Properties

Advanced tunable properties for the Broadcom NetXtreme BCM57XX controller are located in the **space.c** file at **/etc/conf/pack.d/bcme/**. Changing these properties can affect the performance of the driver. Refer to the **bcme man** page for details.

Unexpected Warning Messages

This driver contains a feature that allows the link speed, as reported by **ndstat**, to be updated as the link conditions change.

NOTE: Many warnings messages may be displayed on older UnixWare installations.

If the following warning message is displayed, update your installation.

```
   WARNING: mdi_primitive_handler - Unexpected message from MDI driver(bcme), primitive =
0x17
```

To remove these messages, download and install the latest maintenance pack from the SCO website.

SCO OpenServer Release 5 Driver

Overview

The SCO OpenServer Release 5 driver is released as a media image file containing the driver package. The media image file can be directly copied to the target system for installation, or you can install the media image from a disk.

Creating an Installation Disk

1. Copy the file VOL.000.000 to an SCO system.
2. Create the disk using the following command:
   ```
   dd if=VOL.000.000 of=/dev/rfd0135ds18
   ```

Installing the Driver

1. Use custom or scoadmin software to install the driver from the media image or from the installation disk.
2. After the package is installed, use **netconfig** to add the new network adapter and configure the network protocol and address.
3. After the adapter is added, you can modify the advanced properties to change the settings for the line speed and flow control properties. The advanced properties and their settings are described in Table 2.

Table 2: Advanced Properties

Property	***Setting***	***Comments***
Line Speed	Auto Negotiation (default)	All speeds advertised
	FixedHalfDduplex10	
	AutoHalfDduplex10	Only 10 Mbps speed, half-duplex mode advertised
	FixedFullDduplex10	
	AutoFullDduplex10	Only 10 Mbps speed, full-duplex mode advertised
	FixedHalfDduplex100	
	AutoHalfDduplex100	Only 100 Mbps speed, half-duplex mode advertised
	FixedFullDduplex100	
	AutoFullDduplex100	Only 100 Mbps speed, full-duplex mode advertised
	FixedFullDduplex1000[1]	

Table 2: Advanced Properties (Cont.)

Property	***Setting***	***Comments***
	AutoFullDduplex1000	Only 1 Gbps speed, full-duplex mode advertised
Flow Control	Auto Negotiation[2] Off RxPause TxPause RxPause/TxPause	Symmetric Pause advertised (default)

[1] 1000 Mbps (1 Gbps) full-duplex fixed speed is valid only for fiber connections. For copper twisted-pair connections, 1 Gbps can be set only through auto negotiation with a 1 Gbps link partner.

[2] Auto-negotiation of flow control is valid only when the line speed is set to auto-negotiate (all speeds advertised or single speed advertised).

A kernel rebuild and reboot is required before the new configuration takes effect.

JUMBO FRAMES AND OTHER ADVANCED PROPERTIES

Jumbo MTU sizes and other advanced tunable properties for the Broadcom NetXtreme 57XX controller are located in the space.c file at /etc/conf/pack.d/bcme/. A description of each property is provided in the space.c file. Change the setting of the particular property in the space.c file, rebuild the kernel, and reboot the system. Refer to the **bcme man** page for details.

Windows Driver Software: Broadcom NetXtreme 57XX User Guide

INSTALLING THE DRIVER SOFTWARE

NOTE: If your adapter was installed at the factory, the driver software has been installed for you.

When Windows first starts after a hardware device (such as a Broadcom NetXtreme Gigabit Ethernet adapter) has been installed, or after the existing device driver has been removed, the operating system automatically detects the hardware and prompts you to install the driver software for that device.

Both a graphical interactive installation mode (see Using the Installer) and a command-line silent mode for unattended installation (see Using Silent Installation) are available.

NOTES:

- Before installing the driver software, verify that the Windows operating system has been upgraded to the latest version with the latest service pack applied.
- A network device driver must be installed before the Broadcom NetXtreme Gigabit Ethernet adapter can be used with your Windows operating system. Drivers are located on the installation CD.

Using the Installer

1. **To install the Broadcom NetXtreme drivers**When **Found New Hardware Wizard** opens, click **Cancel**.
2. Insert the installation CD into the CD-ROM or DVD drive.
3. On the installation CD, open the folder for your operating system, open the DrvInst folder, and then double-click Setup.exe file to open the InstallShield Wizard.
4. Click **Next** to continue.
5. After you review the license agreement, click **I accept the terms in the license agreement**, and then click **Next** to continue.
6. Select how you want to install the NetXtreme drivers and then click **Next**.
7. Click **Install**.
8. Click **Finish** to close the wizard.
9. The installer will determine if a system restart is necessary. Follow the on-screen instructions.

Using Silent Installation

NOTES:

- All commands are case sensitive.
- User must “Run as Administrator” for Vista when using “msiexec” for “silent” install/uninstall(s).
- For more detailed instructions and information about unattended installs, refer to the Silent.txt file in the DrvInst folder.

To perform a silent install from within the installer source folder

Type the following:

```
setup /s /v/qn
```

-or-

```
msiexec /i "BDrvInst.msi" /qn
```

To perform a silent upgrade from within the installer source folder

Type the following:

```
setup /s /v/qn
```

To perform a silent uninstall from within the installer source folder

Type the following:

```
msiexec /x "BDrvInst.msi" /qn
```

To perform a silent uninstall from any folder

```
Type the following:
msiexec /x "{B7F54262-AB66-44B3-88BF-9FC69941B643}" /qn
```

To perform a silent reinstall of the same installer

Type the following:

```
setup /s /v"/qn REINSTALL=ALL"
```

To perform a GUI reinstall of the same installer

Type the following:

```
setup /V"REINSTALL=ALL"
```

UPDATING THE DRIVER SOFTWARE

To update the driver software

1. Start Windows and log on. You must have administrative privileges to update the driver software.
2. In Control Panel, click **System** to view **System Properties**.
3. Click the **Hardware** tab, and then click **Device Manager**.
4. Right-click the name of the Broadcom NetXtreme 57XX Gigabit Ethernet Controller and click **Update Driver**.
5. Follow the on-screen instructions provided by the **Hardware Update Wizard**.
6. Click **Include this location in the search**, browse to the folder on the installation CD where the drivers are located, and then click **Next**.
7. Click **Finish** to close the wizard.

REMOVING THE DEVICE DRIVERS

1. Open **Add or Remove Programs** in **Control Panel**.
2. Click **Broadcom NetXtreme Ethernet Controller**, and then click **Remove**.
3. Click **Yes** to remove the drivers and management applications.
4. Restart your system.

NOTE: You can also remove the device drivers by running the InstallShield installer again and clicking **Remove**.

VIEWING OR CHANGING THE PROPERTIES OF THE CONTROLLER

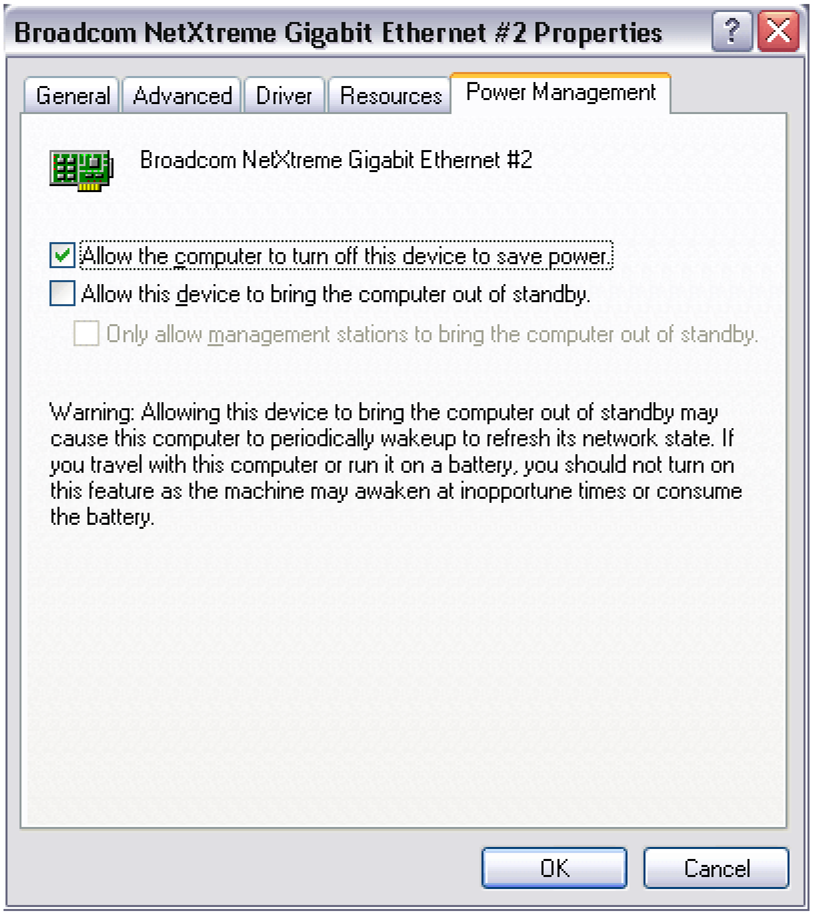
To view or change the properties of the Broadcom NetXtreme 57XX Gigabit Ethernet Controller

1. Right-click the **Control Suite** icon in the taskbar notification area, and then click **Launch BACS**.
2. Click the **Advanced** tab.
3. See Setting Adapter Propertiesfor a detailed description of the available properties as well as for instructions for viewing and changing the value of a particular property.

NOTE: You can also open Broadcom Advanced Control Suite in Control Panel.

Setting Power Management Options

You can set Power Management options to allow the operating system to turn off the adapter to save power or to allow the adapter to wake up the system. If the device is busy doing something (servicing a call, for example) however, the operating system will not shut down the device. The operating system attempts to shut down every possible device only when the system attempts to go into hibernation. To have the adapter stay on at all times, do not select the **Allow the computer to turn off the device to save power** check box.



Broadcom NetXtreme Gigabit Ethernet #2

☑ Allow the computer to turn off this device to save power.

☐ Allow this device to bring the computer out of standby.

☐ Only allow management stations to bring the computer out of standby.

Warning: Allowing this device to bring the computer out of standby may cause this computer to periodically wakeup to refresh its network state. If you travel with this computer or run it on a battery, you should not turn on this feature as the machine may awaken at inopportune times or consume the battery.

NOTES:

- The Power Management tab is available only for systems that support power management.
- To enable Wake on LAN (WOL) when the system is on standby, select the **Allow the device to bring the computer out of standby** check box.
- If you select **Only allow management stations to bring the computer out of standby**, the system can be brought out of standby *only by Magic Packet,* regardless of the settings in **Wake Up Capabilities**.

CAUTION! Do not select the **Allow the computer to turn off the device to save power** check box for any adapter that is a member of a team.

VMware Driver Software: Broadcom NetXtreme 57XX User Guide

PACKAGING

The VMware driver is released in the following packaging format.

Table 1: VMware Driver Packaging

Format	*Drivers*
VMware VIB	vmware-esx-drivers-net-tg3-version.x86_64.vib

DRIVERS

DOWNLOAD, INSTALL, AND UPDATE DRIVERS

To download, install, or update the VMware ESX/ESXi driver for NetXtreme I GbE network adapters, see http://www.vmware.com/support.

DRIVER PARAMETERS

NetQueue

The optional parameter **force_netq** can be used to set the number of Rx and Tx net queues. BCM57XX devices that support NetQueue are the BCM5718, BCM5719, BCM5720, BCM5721, and BCM5722.

By default, the driver tries to use the optimal number of NetQueues. To explicitly force the number of queues, set the number of NetQueues per port via the following command:

```
esxcfg-module -s force_netq=x,x,x.... tg3
```

Allowed values for x are –1 to 15:

- 1–15 will force the number of NetQueues for the given NIC.
- 0 disables NetQueue.
- –1 specifies to use the default driver NetQueue value.

the number of “x” entries can go up to 32, which means the maximum supported NICs = 32.

Example usage:

```
esxcfg-module -s force_netq=-1,0,1,2 tg3]
```

- tg3 NIC 0: Use the default number of NetQueues.
- tg3 NIC 1: Disable the NetQueue feature.
- tg3 NIC 2: Use 1 NetQueue.
- tg3 NIC 3: Use 2 NetQueues.

Note that the NIC # above does not correspond to the vmnic<#>. The NIC number is the system vmnic probe order number. Optimally, the number of NetQueues matches the number of CPUs on the machine.

Driver Parameters

Several optional parameters can be supplied as a command line argument to the vmkload_mod command. These parameters can also be set via the esxcfg-module command. See the man page for more information.

Driver Defaults

Table 2: VMware Driver Defaults

Parameter	*Default Value*
Speed	Autonegotiation with all speeds advertised
Flow Control	Autonegotiation with rx and tx advertised
MTU	1500 (range 46–9000)
Rx Ring Size	200 (range 0–511). Some chips are fixed at 64.
Rx Jumbo Ring Size	100 (range 0–255). Not all chips support the jumbo ring and some chips that suppoort jumbo frames do not use the jumbo ring.
Tx Ring Size	511 (range (MAX_SKB_FRAGS+1) – 511). MAX_SKB_FRAGS varies on different kernels and different architectures. On a 2.6 kernel for x86, MAX_SKB_FRAGS is 18.
Coalesce RX Microseconds	20 (range 0–1023)
Coalesce RX Microseconds irq	20 (range 0–255)
Coalesce rx frames	5 (range 0–1023)
Coalesce rx frames irq	5 (range 0–255)
Coalesce TX Microseconds	72 (range 0–1023)
Coalesce tx usecs irq	20 (range 0–255)
Coalesce tx frames	53 (range 0–1023)
Coalesce tx frames irq	5 (range 0–255)
Coalesce stats usecs	1000000 (aprox. 1 sec.). Some coalescing parameters are not used or have different defaults on some chips.
MSI	Enabled (if supported by the chip and passed the interrupt test).
WoL	Disabled

Driver Messages

The following are the most common sample messages that may be logged in the file /var/log/messages. Use `dmesg -n <level>` to control the level at which messages will appear on the console. Most systems are set to level 6 by default. To see all messages, set the level higher.

Driver Sign On

```
tg3.c:v3.118g (Jan 4, 2012)
```

NIC Detected

```
vmnic0: Tigon3 [partno(BCM95704A6) rev 2003] (PCIX:100MHz:64-bit) MAC address
00:10:18:04:3f:36
vmnic0: attached PHY is 5704 (10/100/1000Base-T Ethernet) (WireSpeed[1])
vmnic0: RXcsums[1] LinkChgREG[0] MIirq[0] ASF[0] TSOcap[1]
vmnic0: dma_rwctrl[769f4000] dma_mask[64-bit]
```

Link Up and Speed Indication

```
tg3: vmnic0: Link is up at 1000 Mbps, full duplex.
tg3: vmnic0: Flow control is on for TX and on for RX.
```

Link Down Indication

```
tg3: vmnic0: Link is down.
```

Installing Management Applications: Broadcom NetXtreme 57XX User Guide

OVERVIEW

The Broadcom Advanced Control Suite version 4 (BACS4) is a management application for configuring the NetXtreme I family of adapters. BACS4 software operates on Windows and Linux server and client operating systems. This chapter describes how to install the BACS4 management application.

There are two main components of the BACS4 utility: the provider component and the client software.

A provider is installed on a server, or “managed host”, that contains one or more CNAs. The provider collects information on the CNAs and makes it available for retrieval from a management PC on which the client software is installed. The client software enables viewing information from the providers and configuring the CNAs.The BACS client software includes a graphical user interface (GUI) and a command line interface (CLI).

COMMUNICATION PROTOCOLS

A communication protocol enables exchanging information between provider and the client software. These are proprietary or open-source implementations of the Web-Based Enterprise Management (WBEM) and Common Information Model (CIM) standards from the Distributed Management Task Force (DMTF). Network administrators can choose the best option based on the prevailing standard on their network.

The following table shows the available options based on the operating systems installed on the managed host and the client.

If the client uses:	*And the managed host uses:*	*BACS can use these communication protocols:*
Windows	Windows	WMI WS-MAN (WinRM)
Windows	Linux	CIM-XML (OpenPegasus) WS-MAN (OpenPegasus)
Linux	Windows	WS-MAN (WinRM)
Linux	Linux	CIM-XML (OpenPegasus) WS-MAN (OpenPegasus)

If the client uses:	*And the managed host uses:*	*BACS can use these communication protocols:*

- WMI = Windows Management Instrumentation.
- WS-MAN = Web Service-Management. WinRM is a Windows-based implementation and OpenPegasus is an open-source implementation of the that operates on Linux.
- CIM-XML = An XML-based version of OpenPegasus.

If your network includes a mix of Windows and Linux clients accessing Windows and Linux servers, then WS-MAN is a suitable choice. If Linux is the only OS installed on the servers, then CIM-XML is an option. If the network includes only Windows servers and clients, WMI is an option. WMI is very simple to configure but is supported only on the Windows OS.

INSTALLATION TASKS

BACS installation includes installing the provider component on the managed host and the client software on the management station. The installation process differs based on the combination of operating systems installed on the client and managed host and on the selected communication protocol. The following sections list each task in the overall process and provide links to the specific steps for each task, as found in Detailed Procedures.

WS-MAN

The following steps install the WS-MAN protocol for communication between the client and managed host (server). WS-MAN is supported on both Windows and Linux clients and servers.

Installing WS-MAN on Windows Server

On Windows servers, configure the WinRM service as follows:

1. Install the WinRM Software Component on Server.
2. Perform Basic Configuration on the Server.
3. Perform User Configuration on the Server.
4. Perform HTTP Configuration on the Server.
5. Perform HTTPS Configuration on the Server (to use HTTPS rather than HTTP)
   a. Generate a Self-Signed Certificate for Windows/Linux Server.
   b. Install the Self-Signed Certificate on Windows Server.
6. Configure WinRM HTTPS/SSL on the Server.
7. Perform Additional Server Configuration, if required.
8. Installing the Broadcom Advanced Control Suite and Related Management Applications.

Installing WS-MAN on Windows Client

On the Windows client, perform following configuration steps.

1. Perform HTTP Configuration (if you plan to use HTTP).
2. Perform HTTPS Configuration (if you plan to use HTTPS).
3. Configure WinRM HTTPS/SSL.
4. Installing the Broadcom Advanced Control Suite and Related Management Applications.

Installing WS-MAN on Linux Server

On Linux server, use the following steps to install OpenPegasus.

1. Install OpenPegasus From Source (Red Hat and SuSE).
2. Start CIM Server on the Server.
3. Configure OpenPegasus on the Server.
4. Install Broadcom CMPI Provider.
5. Perform additional configuration, if required, such as firewall configuration. See Perform Linux Firewall Configuration, If Required.
6. Installing the Broadcom Advanced Control Suite and Related Management Applications.

Installing WS-MAN on Linux Client

To use HTTP, no special configuration is required on the Linux client system. Only the BACS management application must be installed. Perform the following configuration steps:

1. Configure HTTPS on Linux Client.
2. Installing the Broadcom Advanced Control Suite and Related Management Applications.

CIM-XML

CIM-XML is supported only when the server uses the Linux OS. To install CIM-XML on a Linux server and client, you can follow the same procedure as described in WS-MAN. Note, however, that for CIM-XML on the Red Hat Linux OS, two installation options are available:

- Install from the Inbox RPM, as described in Install OpenPegasus From the Inbox RPM (Red Hat Only)
- install from the source RPM, as described in Install OpenPegasus From Source (Red Hat and SuSE).

WMI

The WMI protocol is only supported on Windows OSs. If servers and clients both are running Windows, then WMI can be used.

Installing WMI on Windows server

1. Set up Namespace Security Using WMI Control.
2. Grant DCOM Remote Launch and Activate Permission for a user or group.
3. Perform special configuration if necessary. See Special Configuration for WMI on Different Systems.

Installing WMI on Windows client

No special configuration is required on the Windows client except installing the BACS management application. See Installing the Broadcom Advanced Control Suite and Related Management Applications.

Detailed Procedures

This section provides the step-by-step instructions for each installation task. The required tasks for each communication protocol differ, as listed in Installation Tasks. Refer to the appropriate task list to ensure you complete all necessary tasks for the chosen protocol.

WS-MAN on Windows Server

Install the WinRM Software Component on Server

On the following operating systems, WinRM 2.0 is preinstalled:

- Windows 7
- Windows 8
- Windows 8.1
- Windows Server 2008 R2
- Windows Server 2012
- Windows 2012 R2

For Windows XP and Windows Server, 2008, install Windows Management Framework Core, which includes WinRM 2.0 and Windows Powershell 2.0, from the following link:

http://www.microsoft.com/download/en/details.aspx?displaylang=en&id=11829

Perform Basic Configuration on the Server

The Windows firewall must be enabled for WinRM to work properly. For detailed information about firewall configuration, see Additional Server Configuration. After the firewall is configured, open a command prompt and run the following command to enable the remote management on the Windows server:

```
winrm quickconfig
```

You can use the following command to view the configuration information for the service:

```
winrm get winrm/config
```

Perform User Configuration on the Server

To connect to WinRM, the account must be a member of the local administrators group on the local or remote computer. The output of the `get winrm/config` command will be as follows:

```
RootSDDL = O:NSG:BAD:P(A;;GA;;;BA)S:P(AU;FA;GA;;;WD)(AU;SA;GWGX;;;WD)
```

BA stands for BUILTIN\Administrators.

To add another user group to the WinRM allowed connect list, you can modify the RootSDDL to include the new user group. You will need the SSDL ID for the new group. For example, the following command adds the new user group with SDDL ID S-1-5-21-1866529496-2433358402-1775838904-1021.

```
winrm set winrm/config/Service @{RootSDDL="O:NSG:BAD:P(A;GA;;;BA)(A;;GA;;;
S-1-5-21-1866529496-2433358402-1775838904-1021)S:P(AU;FA;GA;;
WD)(AU;SA;GWGX;;;WD)"}
```

Perform HTTP Configuration on the Server

To use the BACS GUI, you must configure the HTTP protocol, as follows:

NOTE: The default HTTP port is 5985 for WinRM 2.0.

1. Click **Start** (or press the Windows logo key) and select **Run**.
2. Enter **gpedit.msc** to open the local Group Policy editor.
3. Under **Computer Configuration**, open the **Administrative Templates** folder and then open the **Windows Components** folder.
4. Select **Windows Remote Management (WinRM)**.
5. Under **Windows Remote Management (WinRM)**, select **WinRm Client**.
6. Under **WinRM Client**, double-click **Trusted Hosts**.
7. In the **TrustedHostsList**, enter the host names of the clients. If all clients are trusted then enter an asterisk (*) only.
8. Select **WinRM Service**.
9. Enable **Allow Basic Authentication**.
10. Enable **Allow unencrypted traffic**.
11. Close the **Group Policy** wIndow.
12. From the command prompt, run the following command to configure WinRM with default settings:
    ```
    winrm qc or winrm quickconfig
    ```
13. When the tool displays "**Make these changes[y/n]?**", enter "**y**".
14. Enter one of the following commands to check whether an HTTP listener is created:
    ```
    winrm enumerate winrm/confg/listener
    ```
    or
    ```
    winrm e winrm/config/Listener
    ```
15. Enter the following command from the command prompt to test locally.
    ```
    winrm id
    ```

Perform HTTPS Configuration on the Server (to use HTTPS rather than HTTP)

This step consists of two distinct processes: generating a self-signed certificate, if certificate does not exist, and importing it to a Windows server. If one does not already exist, you must configure a self-signed certificate on the Windows server to enable HTTPS/SSL communication with the BACS GUI on the Windows or Linux client. The Windows and Linux client also must be configured with the self-signed certificate. See Perform HTTPS Configuration (if you plan to use HTTPS) to configure Windows and Configure HTTPS on Linux Client to configure Linux client.

NOTE: The self-signed certificate can be created on any Windows or Linux server. The server does not require BACS to be installed. The self-signed certificate generated on any Windows/Linux server should be copied on the local drive of client.

1. Click **Start** (or press the Windows logo key) and select **Run**.
2. Enter **gpedit.msc** to open the local Group Policy editor.
3. Under **Computer Configuration**, open the **Administrative Templates** folder and then open the **Windows Components** folder.

4. Select **Windows Remote Management (WinRM)**.
5. Under **Windows Remote Management (WinRM)**, select **WinRm Client**.
6. Under **WinRM Client**, double-click **Trusted Hosts**.
7. In the **TrustedHostsList**, enter the host names of the clients. If all clients are trusted then enter an asterisk (*) only.
8. Select **WinRM Service**.
9. Enable **Allow Basic Authentication**.

Generate a Self-Signed Certificate for Windows/Linux Server

Openssl on Linux or Windows can be used to generate the self-signed certificate, as follows:

NOTE: You can download and install openssl from http://gnuwin32.sourceforge.net/packages/openssl.htm.

1. Enter the following command to generate a private key:
   ```
   openssl genrsa -des3 -out server.key 1024
   ```
2. You are prompted to enter a passphrase. Be sure to remember the passphrase.
3. Use the following steps to generate a Certificate Signing Request (CSR).

   During the generation of the CSR, you are prompted for several pieces of information. When prompted for the “Common Name”, enter the Windows Server host name or IP address.

   Enter the following command (sample responses are shown):

   ```
   openssl req -new -key server.key -out server.csr
   ```

   If this command does not work, try the following:

   ```
   openssl req -new -key server.key -out server.csr -config openssl.cnf
   ```

   The openssl.cnf file should be placed in the same directory where openssl is placed. Openssl.cnf is located in the folder C:\Program Files (x86)\GnuWin32\share.

   The following information is requested:

   - Country Name (2 letter code) []:**US**
   - State or Province Name (full name) []: **California**
   - Locality Name (e.g., city) []: **Irvine**
   - Organization Name (e.g., company) []: **Broadcom Corporation**
   - Organizational Unit Name (e.g., section) []: **Engineering**
   - Common Name (e.g., YOUR name) []: Enter the host name or IP address of the Windows server. For iPv6, enter the Common Name in the format [xyxy:xxx:….::xxx], **including the brackets [ ]**.
   - (Optional) Email Address []:

   Enter the following additional attributes to be sent with your certificate request:

   - A challenge password []:**linux1**
   - An optional company name []:
4. Remove the passphrase from the key.

   Enter the following commands:

   ```
   cp server.key server.key.org
   openssl rsa -in server.key.org -out server.key
   ```
5. Generate a self-signed certificate:

   To generate a self-signed certificate which is active for 365 days, enter the following command:

```
openssl x509 -req -days 365 -in server.csr -signkey server.key -out server.crt
```

The following output displays:

```
Signature ok
subject=/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/CN=MGMTAPP-
LAB3/emailAddress=
Getting Private key
```

6. Enter the following command to verify the generated self-signed certificate.

```
openssl verify server.crt
```

The following output displays:

```
server.crt:/C=US/ST=California/L=Irvine/O=Broadcom Corporation/OU=Engineering/
CN=MGMTAPP-   LAB3/emailAddress=
error 18 at 0 depth lookup:self signed certificate
OK
```

Ignore the error message “error 18 at 0 depth lookup:self signed certificate”. This error indicates that this is a self-signed certificate.

7. Convert the certificate from "crt" to "pkcs12" format, as follows:

For a Windows server, the certificate should be in pkcs12 format. Enter the following command:

```
openssl pkcs12 -export -in server.crt -inkey server.key -out hostname.pfx
```

You will be prompted for the following:

```
Enter Export Password:
Verifying - Enter Export Password:
```

Enter the password and be sure to remember it. The password is required when importing the certificate on the Windows server and client.

8. Make a copy of the certificate file server.crt and place it on the server where BACS will be installed, so that it can be imported. If you plan to use a Windows or Linux client to connect to the server running BACS, then the certificate also needs to be transferred (copied and pasted) to the client system.

In Linux, the certificate should have the extension “.pem”. The extension “.crt” and “.pem” are the same, so there is no need to use the `openssl` command to convert from .crt to .pem. You can simply copy the file as-is.

NOTE: A separate certificate must be generated for an IPv4 address, IPv6 address, and Hostname.

Install the Self-Signed Certificate on Windows Server

Transfer the file *hostname*.pfx you generated on the Windows server before you install the certificate:

1. Click **Start** (or press the Windows logo key) and select **Run**.
2. Enter **MMC** and click **OK**.
3. Click **File** > **Add/Remove Snap-in**.
4. Click **Add**.
5. Select **Certificates** and click **Add**.
6. Select **Computer account**.
7. Click **Next** and then click **Finish**.
8. Click **Close**, then click **OK**.
9. Open the **Certificates (Local Computer)** folder and then open the **Personal** folder.

10. Right-click **Certificates**, select **All Tasks** and then click **Import**.

11. Click **Next** to begin the Certificate Import Wizard.

12. Browse to select **hostname.pfx**.

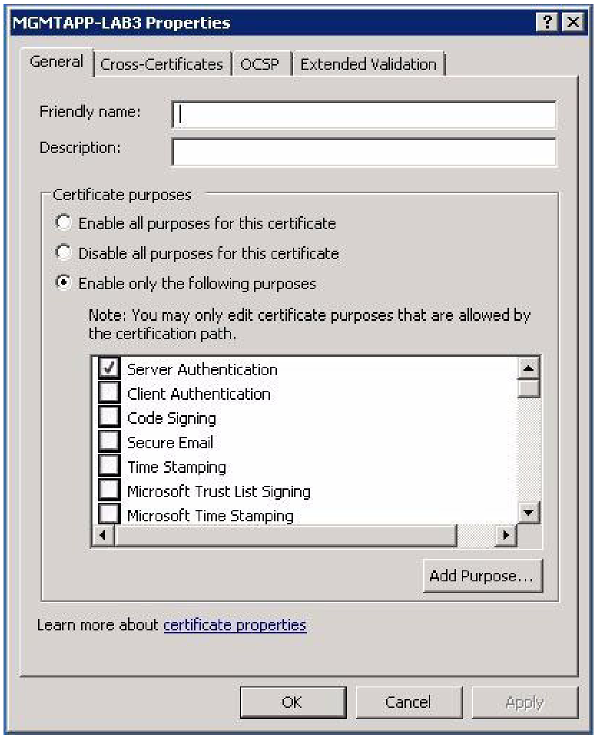
13. When you are prompted for the password for the private key, enter the same password you created in Generate a Self-Signed Certificate for Windows/Linux Server.

14. Follow the instructions, select the defaults, and continue.

The certificate is shown as installed on the right side of the window. The name will be the name you specified while creating a self-signed certificate.

15. Right-click on the certificate and select **Properties**.

A dialog box displays, as follows:



MGMTAPP-LAB3 Properties

General | Cross-Certificates | OCSP | Extended Validation

Friendly name:

Description:

Certificate purposes

○ Enable all purposes for this certificate
○ Disable all purposes for this certificate
● Enable only the following purposes

Note: You may only edit certificate purposes that are allowed by the certification path.

☑ Server Authentication
☐ Client Authentication
☐ Code Signing
☐ Secure Email
☐ Time Stamping
☐ Microsoft Trust List Signing
☐ Microsoft Time Stamping

Add Purpose...

Learn more about certificate properties

OK Cancel Apply

16. Ensure that only **Server Authentication** is enabled, as shown in the figure.

17. Open **Trusted Root Certification Authorities** and then open **Certificates**.

18. Follow the instructions from Step 11. to Step 17.

NOTE: See Perform HTTPS Configuration (if you plan to use HTTPS) for instructions on importing the self-signed certificate on a client.

Configure WinRM HTTPS/SSL on the Server

1. Create WinRM Listener, as follows:

a. Click **Start** (or press the Windows logo key) and select **Run**.

b. Enter **MMC** and click **OK**.

c. Select the self-signed certificate from the Personal store.

For example, if the certificate is created with a host name, the host name will appear.

d. Double-click the certificate to open it.

e. Click the **Details** tab.

f. Scroll down and select the **Thumbprint** field.

g. Select and copy the thumbprint in the **Details** window so you can insert it in the next step.

h. Return to the command prompt.

i. Enter the following command:

```
winrm create winrm/config/Listener?Address=*+Transport=
HTTPS @{Hostname="<HostName or IPAddress>";
CertificateThumbprint="<paste from the previous step and remove the spaces>"}
```

NOTES:

- If the certificate was generated using the host name, enter the host name. If it was generated using the IP address, enter the IP address. For an IPv6 address, use brackets [ ] around the address.
- If HTTPS is configured in your system, the listener must be deleted before creating a new HTTPS listener. Use the following command:
  ```
  winrm delete winrm/config/Listener?Address=*+Transport=HTTPS
  ```

j. The above command creates a listener on the HTTPS port (5986) using any/all network address of the server, and my SelfSSL generated certificate.

k. You can use the `winrm` command to modify or set the HTTPS listener, as WinRM listeners can be configured on any user defined port.

l. From command prompt, run the following command to verify that the listener(s) that have been configured:

```
winrm e winrm/config/listener
```

2. Test HTTPS/SSL connection on the server.

a. At the command prompt on the server, enter the following command:

```
winrs -r:https://yourserver:5986 -u:username -p:password hostname
```

b. If setup correctly, the output of the command shows the server host name.

c. To check WinRM Service Configuration, run the following command:

```
winrm get winrm/config/service
```

Additional Server Configuration

If necessary, modify the firewall rules as follows:

Windows Server 2008 R2

1. From the **Administrative Tools** menu, open **Windows Firewall with Advanced Security**.
2. Right-click **Inbound Rules** and select **New Rule**.

   The new rule wizard opens.
3. Select **Port** and click **Next**.
4. On the **Protocol and Ports** screen, select **TCP** and enter the specific port, for example, 5985 for HTTP or 5986 for HTTPS.
5. Click **Next**.
6. On the **Action** screen, select **Allow the connection** and click **Next**.
7. For **Profile**, you can select all three profiles if your server is in a workgroup.

8. Specify a name for the rule and click **Finish**.
9. Ensure that the new rule and is enabled (the green check box is selected).

Windows XP

1. Click **Start** > **Control Panel**, and then double-click **Windows Firewall**.
2. Click the **Exceptions** tab
3. Click **Add Port**.
4. Enter a meaningful **Name**, for example "WinRM rule" and port number, for example, 5985 for HTTP or 5986 for HTTPS.
5. Click **OK**.

Useful WinRM Commands

Command	***Description***
`winrm quickconfig` or `winrm qc`	Configures WinRM with default settings
`winrm enumerate winrm/config/Listener` or `winrm e winrm/config/Listener`	Helps to check which service listener are enabled and listening on which port and IP Address.
`winrm get winrm/config/Service`	Checks WinRM Service Configuration.
`winrm delete winrm/config/Listener?Address=*+Transport=HTTPS`	Deletes a Listener (in this case deleting a HTTPS listener).

Useful WinRM Websites

- http://msdn.microsoft.com/en-us/library/aa384372%28v=vs.85%29.aspx
- http://support.microsoft.com/kb/968929
- http://blogs.technet.com/b/jonjor/archive/2009/01/09/winrm-windows-remote-management-troubleshooting.aspx
- http://support.microsoft.com/kb/2019527
- http://technet.microsoft.com/en-us/library/cc782312%28WS.10%29.aspx
- http://msdn.microsoft.com/en-us/library/aa384295%28v=VS.85%29.aspx

WS-MAN—WINDOWS CLIENT

Perform HTTP Configuration (if you plan to use HTTP)

1. Click **Start** (or press the Windows logo key) and select **Run**.
2. Enter **gpedit.msc** to open the local Group Policy editor.
3. Under **Computer Configuration**, open the **Administrative Templates** folder and then open the **Windows Components** folder.
4. Select **Windows Remote Management (WinRM)**.
5. Under **Windows Remote Management (WinRM)**, select **WinRm Client**.
6. Under **WinRM Client**, double-click **Trusted Hosts**.
7. In the **TrustedHostsList**, enter the host names of the clients and click **OK**. If all clients are trusted then enter an asterisk (*) only.
8. Select **WinRM Service**.
9. Enable **Allow Basic Authentication** and click **OK**.
10. Run the following command from the command prompt to test the connection:
    ```
    winrm id -remote:<remote machine Hostname or IP Address>
    ```

Perform HTTPS Configuration (if you plan to use HTTPS)

After you generate a self-signed certificate, as described in Generate a Self-Signed Certificate for Windows/Linux Server, you can import the certificate on the client to facilitate a connection between server and client. Ensure that all steps mentioned in section Generate a Self-Signed Certificate for Windows/Linux Server are completed, including copying *hostname.pfx* at the location from where client can access it, before you proceed with the following steps.

1. Click **Start** (or press the Windows logo key) and select **Run**.
2. Enter **MMC** and click **OK**.
3. Click **File** and select **Add/Remove Snap-in**.
4. Click **Add**.
5. Select **Certificates** and click **Add**.
6. Select **Computer account** and click **Next**.
7. Click **Finish**.
8. Click **Close** and then click **OK**.
9. Under **Certificates (Local Computer)**, right-click on **Trusted Root Certification Authorities**, select **All Tasks**, and select **Import**.
10. Click **Next** to begin the Certificate Import Wizard.
11. Browse to select the .pfx file you generated in Generate a Self-Signed Certificate for Windows/Linux Server. Change the selection in the **Files of type** list to **Personal Information Exchange (*.pfxas, *.p12)**, select the *hostname.pfx* file and click **Open**.
12. Enter the password you assigned to the private key and click **Next**.

Configure WinRM HTTPS/SSL

You can run `winrm` from a client to retrieve information from the server using WinRM HTTPS connection. Use the following steps to test the WinRM HTTPS/SSL connection from client:

1. To retrieve the server operating system information, enter the following command.
   ```
   winrm e wmi/root/cimv2/Win32_OperatingSystem -r:https://yourservername
   -u:username -p:password -skipCAcheck
   ```
2. To retrieve the server WinRM identity information, enter the following command.
   ```
   winrm id -r:https://yourservername -u:username -p:password -skipCAcheck
   ```
3. To enumerate Windows services on the server, enter the following command.
   ```
   winrm e wmicimv2/Win32_service -r:https://yourservername -u:username -p:password -skipCAcheck
   ```

NOTE: It is important to use `-skipCAcheck` switch in the `winrm` command line testing, as the certificate is self-generated and not imported on the client. Otherwise, the following error message displays: `WSManFault`.

The next section explains how to export and import the self-signed certificate.

WS-MAN AND CIM-XML—LINUX SERVER

There are two options available for installing OpenPegasus: install from an Inbox RPM or install from the source. The Inbox OpenPegasus is available only on the Red Hat Linux OS. For the SUSE Linux Enterprise Server 11 (SLES11) OS, you must use the source RPM.SLES11,

NOTE: The Inbox RPM does not support the WS-MAN communication protocol. To use WS-MAN, you must install OpenPegasus from source.

Install OpenPegasus From the Inbox RPM (Red Hat Only)

In Red Hat Linux, an Inbox OpenPegasus RPM is available as `tog-pegasus-<version>.<arch>.rpm`.

1. Use the following command to install tog-pegasus:
   ```
   rpm -ivh tog-openpegasus-<version>.<arch>.rpm
   ```
2. Use the following command to start Pegasus:
   ```
   /etc/init.d/tog-pegasus start
   ```

NOTE: If your system has “Red Hat Security Enhancement for tog-pegasus” enabled, disable it before connecting to BACS. See /usr/share/doc/tog-pegasus-2.5.2/README.RedHat.Security for details. To disable it, remove the line from /etc/pam.d/wbem.

NOTE: On SuSE Linux, the Inbox OpenPegasus RPM is not available. OpenPegasus must be installed from source, as described in the following section.

Note that in inbox Pegasus, HTTP is not enabled by default. After Inbox OpenPegasus is installed successfully, if no further configuration is required, then follow the instructions in Install Broadcom CMPI Provider. To enable HTTP, see Enable HTTP.

Install OpenPegasus From Source (Red Hat and SuSE)

The OpenPegasus source can be downloaded from www.openpegasus.org.

NOTE: If not already installed, download and install the openssl and libopenssl-devel rpm. This step is optional and required only if you are planning to use HTTPS to connect the client to the managed host.

Set the Environment Variable

Set the environment variables for building OpenPegasus as follows.

Environment Variable	*Description*
PEGASUS_ROOT	The location of the Pegasus source tree
PEGASUS_HOME	The location for the built executable, repository; e.g., $PEGASUS_HOME/bin, PEGASUS_HOME/lib, $PEGAUS_HOME/repository, and $PEGASUS_HOME/mof subdirectories.
PATH	$PATH:$PEGASUS_HOME/bin
PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER	True
PEGASUS_CIM_SCHEMA	"CIM222"
PEGASUS_PLATFORM	For Linux 32 bit systems: "LINUX_IX86_GNU" For Linux 64 bit systems: "LINUX_X86_64_GNU"
PEGASUS_HAS_SSL	Optional. Set to "true" for HTTPS support.
PEGASUS_ENABLE_PROTOCOL_WSMAN	Optional. Set to "true" for WSMAN protocol support.

Additional Settings

The $PEGASUS_HOME variable must be set up in the shell environment, and $PEGASUS_HOME/bin needs to be appended to the $PATH environment.

Examples

- export PEGASUS_PLATFORM="LINUX_X86_64_GNU"
- export PEGASUS_CIM_SCHEMA="CIM222"
- export PEGASUS_ENABLE_CMPI_PROVIDER_MANAGER=true
- export PEGASUS_ROOT="/share/pegasus-2.10-src"
- export PEGASUS_HOME="/pegasus"
- export PATH=$PATH:$PEGASUS_HOME/bin

For SSL Support, add the following environment variable:

- export PEGASUS_HAS_SSL=true

For WS-MAN Support, add the following environment variable:

- export PEGASUS_ENABLE_PROTOCOL_WSMAN=true

CIM-XML and WSMAN in OpenPegasus use the same ports for HTTP or HTTPs. The default port numbers for HTTP and HTTPS are 5989 and 5989, respectively.

NOTE: You can add these exports at the end of the .bash_profile. This file is located in the /root directory.

- The environment variables will be set when a user logs in using PuTTY.
- On the Linux system itself, for each terminal where the environment variables are not set, run the following command:
  ```
  source /root/.bash_profile
  ```
- When you logout and login, the environment variables will be set.

Build and install OpenPegasus

From $PEGASUS_ROOT (the location of the Pegasus source root directory), run the following:

```
make clean
make
make repository
```

NOTE: Whenever OpenPegasus is built from source, all configurations are reset to the default values. If you are rebuilding OpenPegasus, you must redo the configuration as mentioned in Configure OpenPegasus on the Server.

Start CIM Server on the Server

Use the `cimserver` command to start CIM server. To stop CIM server, use the command `cimserver -s`.

To check whether OpenPegasus has been installed properly, enter the following command:

```
cimcli ei -n root/PG_Interop PG_ProviderModule
```

NOTE: For OpenPegasus compiled from source, PEGASUS_HOME must be defined when you start CIM server. Otherwise, CIM server will not load the repository properly. Consider setting PEGASUS_HOME in the ".bash_profile" file.

Configure OpenPegasus on the Server

Use the `cimconfig` command to configure OpenPegasus, as shown in the following table:

Command	***Description***
`cimconfig -l`	List all valid property names.
`cimconfig -l -c`	List all valid property names and its value
`cimconfig -g <property name>`	Query a particular property.
`cimconfig -s <property name>=<value> -p`	Set a particular property.
`cimconfig --help`	Find out more about the command.

CIM server must be started before running `cimconfig`, and must be restarted for configuration changes to take effect.

Enable Authentication

The following OpenPegasus properties have to be set as described in this section. Otherwise, the Broadcom CIM Provider will not work properly. Ensure the following are set before launching BACS and connecting to the provider.

Start CIM server if it is not already started. Then, set the following:

- `cimconfig -s enableAuthentication=true -p`
- `cimconfig -s enableNamespaceAuthorization=false -p`
- `cimconfig -s httpAuthType=Basic -p`
- `cimconfig -s passwordFilePath=cimserver.passwd -p`
- `cimconfig -s forceProviderProcesses=false -p`

If you want root user to connect remotely:

- `cimconfig -s enableRemotePrivilegedUserAccess=true -p`

User configuration with privilege: The Linux system users are used for OpenPegasus authentication. The systems users have to be added to OpenPegasus using `cimuser` to connect via BACS:

- `cimuser -a -u` *<username>* `-w` *<password>*

  Example: `cimuser -a -u root -w linux1`

Enable HTTP

1. If CIM server is not started, start it.
2. Use the following command to set up an HTTP port (optional):
   `cimconfig -s httpPort=5988 -p`

   This property is not available for Inbox OpenPegasus.
3. Use the following command to enable HTTP connection:
   `cimconfig -s enableHttpConnection=true -p`
4. Use the `cimserver -s` and `cimserver` commands, respectively, to stop and restart CIM server for the new configuration to take effect.

Enable HTTPS

1. If CIM server is not started, start it.
2. Set up HTTPS port with the following command (optional):
   `cimconfig -s httpsPort=5989 -p`

This property is not available for inbox OpenPegasus.

3. Enable HTTPS connection with 'the following command:
   `cimconfig -s enableHttpsConnection=true -p`
4. Use the `cimserver -s` and `cimserver` commands, respectively, to stop and restart CIM server for the new configuration to take effect.

Install Broadcom CMPI Provider

Ensure that OpenPegasus is installed properly before installing CMPI Provider.

Install

Enter following command to install Broadcom CMPI Provider.

```
% rpm -i BRCM_CMPIProvider-{version}.{arch}.rpm
```

Uninstall

Enter following command to uninstall Broadcom CMPI Provider:

```
% rpm -e BRCM_CMPIProvider
```

Perform Linux Firewall Configuration, If Required

Follow these procedures to open the appropriate ports in the firewall:

RedHat

1. Click **System**, select **Administration**, and then select **Firewall**.
2. Select **Other Ports**.
3. In the Port and Protocol Dialog box, select **User Defined**.
4. In the **Port/Port Range** field, add the port number.
5. In the **Protocol** field, add the protocol as TCP or UDP, etc.
6. Click **Apply** for the firewall rules to take effect.

Example:

- For CIM-XML over HTTP, the port number is 5988 and protocol is TCP.
- For CIM-XML over HTTPs, the port number is 5989 and protocol is TCP.

SuSE

1. Click **Compute** and then click **YaST**.
2. Select **Security & Users** on the left pane.
3. On the right pane, double-click **Firewall**.
4. Select **Custom Rules** on the left pane.
5. On the right pane click **Add**.
6. Enter the following values:
   - **Source Network**: 0/0 (means all)
   - **Protocol**: TCP (or the appropriate protocol)
   - **Destination Port**: *<Port Number>* or *<Range of Port Numbers>*
   - **Source Port**: Leave blank.
7. Click **Next** and then click **Finish** for the firewall rules to take effect.

Example:

For CIM-XML, use the following values:

- **Source Network**: 0/0 (means all)
- **Protocol**: TCP
- **Destination Port**: 5988:5989

- **Source Port**: Leave blank.

WS-MAN AND CIM-XML—LINUX CLIENT

No special software components are required on the Linux client system to use the HTTP except installing the BACS management application. However, for WS-MAN installations, you can optionally configure the HTTPS protocol for use with BACS.

Configure HTTPS on Linux Client

Follow these steps if you want to use HTTPS rather than HTTP (WS-MAN only):

1. Follow the instructions in Generate a Self-Signed Certificate for Windows/Linux Server.
2. Import Self-Signed Certificate on Linux Client:

   On Linux distributions, note the following certificate directory:

   - For all SuSE versions, the certificate directory is `/etc/ssl/certs`.
   - For RedHat, the certificate directory can be different for each version. For some versions, it is `/etc/ssl/certs` or `/etc/pki/tls/certs`. For other versions, find out the certificate directory.

   Copy *hostname.pem*, which you created in Generate a Self-Signed Certificate for Windows/Linux Server, into the certificate directory of the Linux client. For example, if the certificate directory is `/etc/ssl/certs`, copy *hostname.pem* to `/etc/ssl/certs`.

   a. Change directory to `/etc/ssl/certs`.

   b. Create a hash value by running the following command.

   ```
   openssl x509 -noout -hash -in hostname.pem
   ```

   A value such as the following will be returned.

   ```
   100940db
   ```

   c. Create a symbolic link to the hash value by running the following command:

   ```
   ln -s hostname.pem 100940db.0
   ```

3. Test HTTPS/SSL Connection from Linux Client

   Use the following command to test whether the certificate is installed correctly on Linux:

   ```
   # curl -v --capath /etc/ssl/certs https://Hostname or IPAddress:5986/wsman
   ```

   If this fails, then the certificate is not installed correctly and an error message displays, indicating to take corrective action.

Install BACS Management Application

1. Download the latest BACS management application RPM package.
2. Install the RPM package as:
   ```
   rpm -i BACS-{version}.{arch}.rpm
   ```

WMI—WINDOWS

Perform the steps in the following two sections only to configure WMI on the Windows server.

Set up Namespace Security Using WMI Control

The WMI Control provides one way to manage namespace security. You can start the WMI Control from the command prompt using this command:

```
wmimgmt
```

On Windows 9x or Windows NT4 computers that have WMI installed, use this command instead:

```
wbemcntl.exe
```

Alternatively, you can access the WMI Control and the Security tab as follows:

1. Right-click on **My Computer** and click **Manage**.
2. Double-click **Services and Applications** and then double-click **WMI Control**.
3. Right-click **WMI Control** and then click **Properties**.
4. In WMI Control Properties, click the **Security** tab.
5. A folder named Root with a plus sign (+) next to it should now be visible. Expand this tree as necessary to locate the namespace for which you want to set permissions.
6. Click **Security**.

   A list of users and their permissions appears. If the user is on the list, modify the permissions as appropriate. If the user is not on the list, click **Add** and add the user from the location (local machine, domain, etc.) where the account resides.

NOTES: You can add these exports at the end of the .bash_profile. This file is located in the /root directory.

- In order to view and set namespace security, the user must have Read Security and Edit Security permissions. Administrators have these permissions by default, and can assign the permissions to other user accounts as required.
- If this user needs to access the namespace remotely, you must select the Remote Enable permission.
- By default, user permissions set on a namespace apply only to that namespace. If you want the user to have access to a namespace and all subnamespaces in the tree below it, or in subnamespaces only, click **Advanced**. Click **Edit** and specify the scope of access in the dialog box that displays.

Grant DCOM Remote Launch and Activate Permission

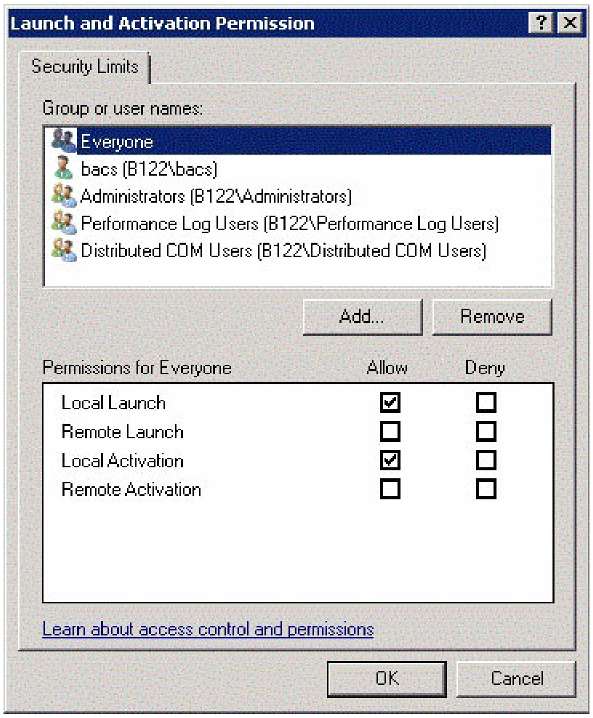
In the Windows domain environment, the Domain Administrator account has the necessary privilege level to access the WMI component for BACS management and, therefore, no special configuration is needed. In a large enterprise, however, a user who is accessing the local or remote host using the BACS4 client GUI may not always have the domain administrator account privilege. It is necessary to configure WMI security access on the remote host to allow the user to connect to it using the BACS4 client GUI.

This configuration can be easily done using the following procedure. If you do not have sufficient privileges to configure security for WMI access, contact your Network Administrator.

1. Click **Start** (or press the Windows logo key) and select **Run**.
2. Enter **DCOMCNFG**, and then click **OK**.

3. The Component Services dialogue box displays.
4. Open **Component Services** and then open **Computers**.
5. Right-click **My Computer** and click **Properties**.
6. In **My Computer Properties**, click the **COM Security** tab.
7. Under **Launch and Activation Permissions**, click **Edit Limits**.
8. Follow these steps if your name or your group does not appear in the **Groups or user names** list.
   a. In the Launch Permission dialog box, click **Add**.
   b. In the Select Users, Computers, or Groups dialog box, add your name and the group in the **Enter the object names to select** box, and then click **OK**.
   c. In the Launch Permission dialog box, select your user and group in the **Group or user names** list.
   d. In the **Permissions for User** area, select **Allow** for **Remote Launch** and **Remote Activation**, and then click **OK**.

Figure 1: Launch and Activation Permission



Launch and Activation Permission

Security Limits

Group or user names:

- Everyone
- bacs (B122\bacs)
- Administrators (B122\Administrators)
- Performance Log Users (B122\Performance Log Users)
- Distributed COM Users (B122\Distributed COM Users)

Permissions for Everyone	Allow	Deny
Local Launch	☑	□
Remote Launch	□	□
Local Activation	☑	□
Remote Activation	□	□

Learn about access control and permissions

For more information, see Securing a Remote WMI Connection on the Microsoft Developer Network site.

Special Configuration for WMI on Different Systems

- On a Windows XP Pro computer, ensure that remote logons are not being coerced to the GUEST account (referred to as “ForceGuest”, which is enabled by default on computers that are not attached to a domain). Open the Local Security Policy editor by clicking **Start** > **Run** and entering **secpol.msc**. Open the **Local Policies** node and select **Security Options**. Then, scroll down to the setting titled **Network access: Sharing and security model for local accounts**. If this is set to **Guest only**, change it to **Classic** and restart the computer.
- In Windows Vista and Windows 7, in order to let all users in the administrator group connect using the WMI namespace, the user might need to change the LocalAccountTokenFilterPolicy as needed.

INSTALLING THE BROADCOM ADVANCED CONTROL SUITE AND RELATED MANAGEMENT APPLICATIONS

INSTALLING ON A WINDOWS SYSTEM

The Broadcom Advanced Control Suite (BACS) software and related management applications can be installed from the installation CD or by using the silent install option.

The following are installed when running the installer:

- **Control Suite**. Broadcom Advanced Control Suite (BACS). If selected, a GUI and a CLI client are installed.
- **BASP**. Broadcom Advanced Server Program. This is a Broadcom intermediate NDIS driver to configure VLAN, Team, Load Balancing etc.
- **SNMP**. The Simple Network Management Protocol subagent. This feature allows the SNMP manager to monitor the Broadcom Network Adapters.
- **CIM Provider**. Common Information Model provider. This component presents the network adapter information to WMI based management applications. Select this component on a host which has Broadcom adapter installed and which you want to manage using the GUI client.

NOTES:

- Ensure that the Broadcom network adapter(s) is physically installed in the system before installing BACS.
- Before you begin the installation, close all applications, windows, or dialog boxes.
- BASP is not available on Windows Small Business Server (SBS) 2008.

Using the Installer

To install the management applications

1. Insert the installation CD into the CD or DVD drive.
2. On the installation CD, open the MgmtApps folder, select IA32 or x64, and then double-click **Setup.exe** to open the InstallShield Wizard.
3. Click **Next** to continue.
4. After you review the license agreement, click **I accept the terms in the license agreement** and then click **Next** to continue.
5. Select the features you want installed.
6. Click **Next**.
7. Click **Install**.
8. Click **Finish** to close the wizard.

After successful installation, you can start the GUI from Windows Start menu.

Using Silent Installation

NOTES:

- All commands are case sensitive.
- User must “Run as Administrator” for Vista when using “msiexec” for “silent” install/uninstall(s).
- For detailed instructions and information about unattended installs, refer to the Silent.txt file in the MgmtApps folder.

To perform a silent install (or upgrade) from within the installer source folder

Type the following:

```
setup /s /v/qn
```

If performing a silent upgrade, your system may reboot automatically. To suppress the reboot, type the following:

```
setup /s /v"/qn REBOOT=ReallySuppress"
```

To perform a silent install and create a log file

Type the following:

```
setup /s /v"/qn /L f:\ia32\1testlog.txt"
```

The 1testlog.txt log file will be created at f:\ia32.

To perform a silent uninstall from any folder on the hard drive

```
msiexec /x "{26E1BFB0-E87E-4696-9F89-B467F01F81E5}" /qn
```

NOTES:

- The hexadecimal number above may differ from your current installer. Check the Key name corresponding with the Broadcom Advanced Control Suite (BACS) application in HKLM\Software\Microsoft\Windows\CurrentVersion\Uninstall for the correct hexadecimal number.
- After performing a silent uninstall, it is necessary to reboot the system before reinstalling this installer. If a reboot is not performed, BASP will not install correctly.

To perform a silent install by feature on IA32 platforms

Use ADDSOURCE to include any of the features listed below.

NOTE: CHM32 or CHM64 installs the BACS help file and must be included when installing the BACS feature.

```
setup /s /v"/qn ADDSOURCE=BACSi32,CHM32,BASPi32,SNMPi32,CIMi32"
```

To perform a silent install by feature on AMD64/EM64T platforms

Type the following:

```
setup /s /v"/qn ADDSOURCE=BACSa64,CHMa64,BASPa64,SNMPa64"
```

To perform a silent install from within a batch file

To perform a silent install from within a batch file and wait for the install to complete before continuing with the next command line, type the following:

```
start /wait setup /s /w /v/qn
```

INSTALLING ON A LINUX SYSTEM

The Broadcom Advanced Control Suite (BACS) software can be installed on a Linux system using the Linux RPM package. This installation includes a BACS GUI and a CLI client.

Before you begin:

- Ensure that the Broadcom network adapter(s) is physically installed and the appropriate device driver for the NICis is installed on the system to be managed by this utility.
- Ensure that the CIM provider is installed properly on the system that is to be managed by this utility. See
- For managing iSCSI on Linux hosts, ensure that the open-iscsi and sg utilities are installed on the Linux host.

To install BACS

1. Download the latest BACS management application RPM package.
2. Install the RPM package using the following command:
   ```
   % rpm -i BACS-{version}.{arch}.rpm
   ```

To Use BACS

- To use the GUI, on XWindow, double-click the BACS4 desktop icon, or access the BACS program from the task bar under **System Tools**.
- To use BACS CLI, refer to the file BACSCLI_Readme.txt provided with the release files.

To remove BACS

To uninstall the RPM package, use the following command:

```
% rpm -e BACS
```

MANAGING MANAGEMENT APPLICATIONS (WINDOWS)

MODIFYING THE MANAGEMENT APPLICATION

To modify the management applications:

1. In Control Panel, double-click **Add or Remove Programs**.
2. Click **Broadcom Management Programs** and then click **Change**.
3. Click **Next** to continue.
4. Click **Modify** to change program features.
5. Click **Next** to continue.
6. Click on an icon to change how a feature is installed.
7. Click **Next**.
8. Click **Install**.
9. Click **Finish** to close the wizard.
10. Reboot your system to complete the modification of the management applications.

REPAIRING MANAGEMENT APPLICATIONS

To repairthe management applications:

1. In Control Panel, double-click **Add or Remove Programs**.
2. Click **Broadcom Management Programs**, and then click **Change**.
3. Click **Next** to continue.
4. Click **Repair** to repair errors in installed applications.
5. Click **Next** to continue.
6. Click **Install**.
7. Click **Finish** to close the wizard.

REMOVING MANAGEMENT APPLICATIONS

To remove all management applications:

1. In Control panel, double-click Add or Remove Programs.
2. Click **Broadcom Management Programs**, and then click **Remove**.
3. Reboot your system to complete the removal of management applications.

To remove the management application using the CLI:

Enter following command:

```
rpm -e BACS
```

Using Broadcom Advanced Control Suite 4: Broadcom NetLink®/NetXtreme® 57XX User Guide

Broadcom Advanced Control Suite Overview

Broadcom Advanced Control Suite (BACS) is an integrated utility that provides useful information about each network adapter that is installed in your system. BACS also enables you to perform detailed tests, diagnostics, and analyses on each adapter, as well as to view and modify property values and view traffic statistics for each network object.

Broadcom Advanced Server Program (BASP), which runs within Broadcom Advanced Control Suite, is used to configure teams for load balancing, fault tolerance, and virtual local area networks (VLANs). BASP functionality is available only on systems that use at least one Broadcom network adapter.

Starting Broadcom Advanced Control Suite

In Control Panel, click **Broadcom Control Suite 4,** or click the BACS icon in the taskbar located at the bottom of the Windows desktop.

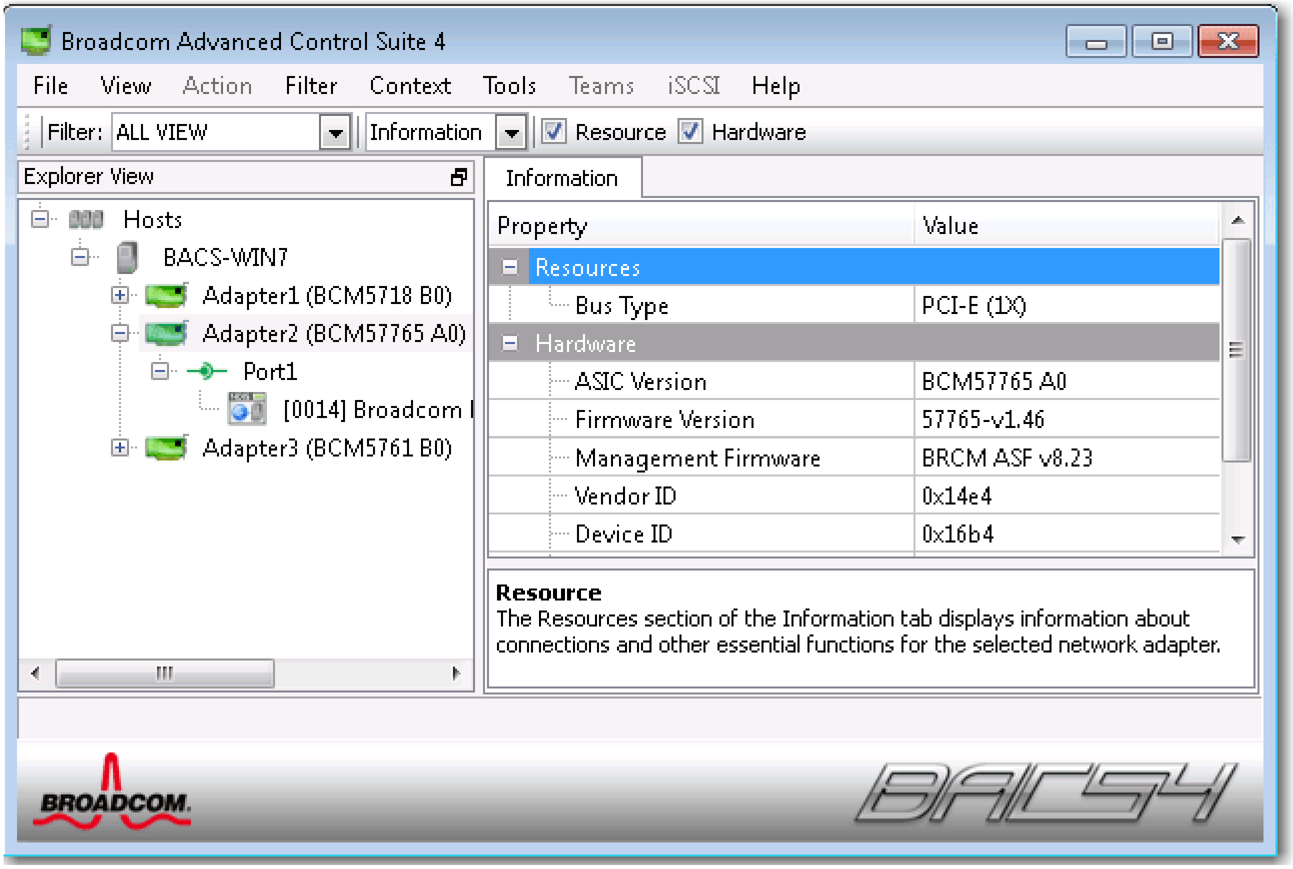
On Linux systems, you can double-click the BACS4 desktop icon, or access the BACS program from the task bar under **System Tools**. (If you are having difficulty launching BACS on a Linux system, see the related topic in Troubleshooting BACS.)

BACS Interface

The BACS interface is comprised of the following regions:

- Explorer View pane
- Context View selector
- Context View pane
- Menu bar
- Description pane

By default, the Explorer View pane is docked and pinned on the left side of the main window, the Context View pane on the right, the Context View selector below the menu bar, and the Description pane below the Context View pane. Drag the splitter between any two panes to vary the size of the panes.



Property	Value
⊟ Resources	
Bus Type	PCI-E (1X)
⊟ Hardware	
ASIC Version	BCM57765 A0
Firmware Version	57765-v1.46
Management Firmware	BRCM ASF v8.23
Vendor ID	0x14e4
Device ID	0x16b4

Resource
The Resources section of the Information tab displays information about connections and other essential functions for the selected network adapter.

Explorer View Pane

You can dock and pin the Explorer View pane on the left side, right side, top, or bottom of the main window.

The Explorer View pane lists the objects that can be viewed, analyzed, tested, or configured by BACS. When an item is selected in the Explorer View pane, the tabs showing the information and options that are available for the item appear in the Context View pane.

The organization of this panel is designed to present the manageable objects in the same hierarchical manner as drivers and its subcomponents. This simplifies the management of various elements of the network interface controller (NIC). The top level of the hierarchy is the Host container, which lists all hosts managed by BACS. Below the hosts are the installed network adapters, with the manageable elements, such as physical port, VBD, and NDIS below the adapters.

The icon next to each device in the Explorer View pane shows its status. An icon next to a device name that appears normal means the device is connected and working.

- **X.** A red “X” that appears on the device’s icon indicates the device is currently not connected to the network.
- **Greyed out.** A device icon that appears greyed out indicates the device is currently disabled.

Context View Selector

The Context View selector appears below the menu bar and includes the filter and tab categories. Although you can expand and collapse the categories that appear on tabs in the Context View pane, you can alternatively display a category by selecting the box next to the category name.

Filter View

In a multiple-host environment using several network adapters, there can be a large number of manageable elements per adapter that can be difficult and cumbersome to view, configure, and manage all elements. Use the filter to select a particular device function. Possible filter views include:

- All
- Team view
- NDIS view
- iSCSI view
- FCoE view
- iSCSI Target view
- FCoE Target view
- TruManage view

Context View Pane

The Context View pane displays all the parameters that you can view for the object selected in the Explorer View pane. The parameters are grouped by tabs and categories, depending on the parameter type. The available tabs are Information, Configuration, Diagnostics, and Statistics. Because the BACS interface is context-sensitive, only the parameters that apply to the selected object can be viewed or configured in the Context View pane.

Menu Bar

The following appear on the menu bar, but because the menu items are context-sensitive, not all items will be available at all times:

File menu

- Team Save As: Saves the current team configurations to a file
- Team Restore: Restores any saved team configuration from a file

Action menu

- Remove Host: Removes the selected host
- Refresh Host: Refreshes the information for the selected host

View menu

- Explorer View: Displays/hides the Explorer View pane
- Tool Bar: Displays/hides the tool bar
- Status Bar: Displays/hides the status bar
- Broadcom Logo: Displays/hides the Broadcom Logo on BACS to optimize the maximum viewable space

Tools menu

- Options: Used for configuring BACS preferences

Teams

- Create Teams: Creates new teams with either the Teaming Wizard or in Advanced mode
- Manage Teams: Manages existing teams with either the Teaming Wizard or in Advanced mode

Description Pane

The Description pane provides information, configuration instructions, and options for the selected parameter in the Context View pane.

CONFIGURING PREFERENCES

To enable or disable the BACS tray icon

BACS places an icon in the Windows taskbar when the program is installed. Use the Options window to turn this icon on or off.

1. From the **Tools** menu, select **Options**.
2. Select or clear **Enable BACSTray** (the option is enabled by default).
3. Click **OK**.

Setting the teaming mode

1. From the **Tools** menu, select **Options**.
2. Select **Expert Mode** if you do not need the assistance of the teaming wizard to create teams; otherwise, select **Wizard Mode**.
3. Click **OK**.

Setting the Explorer View refresh time

1. From the **Tools** menu, select **Options**.
2. Select **Auto** to set the Explorer View refresh time to 5 seconds. Otherwise, select **Custom** and select a time, in seconds.
3. Click **OK**.

CONNECTING TO A HOST

You can add one or more Windows or Linux hosts to manage from BACS.

To add a local host

1. From the **Action** menu, click **Add Host**.
2. For both Windows and Linux hosts, do not change the default settings. The **User name** and **Password** are not required while connecting to the local host.
3. Select **Persist** if you want BACS to save the information for this host.
4. Click **Ok**. BACS can now be used to view information and manage the host.

To add a remote host

1. From the **Action** menu, click **Add Host**.
2. Type the remote host's name or IP address in the **Host** box.
3. Select the protocol from the **Protocol** list. The protocol options for Windows are **WMI**, **WSMan**, or **Try All**. The protocol options for Linux are **CimXML**, **WSMan**, or **Try All**. The **Try All** option forces the GUI client to try all options.
4. Select the **HTTP** scheme, or the **HTTPS** scheme for added security.
5. Type the **Port Number** value you used to configure the host, if it is different than the default value of **5985**.
6. Type the **User name** and **Password**.
7. Select **Persist** if you want BACS to save the information for this host. The host will appear in the Explorer Pane whenever you reopen BACS, and you will not need to enter the host IP address or host name when connecting to the host. For security reasons, you must enter the **User name** and **Password** every time.
8. Click **OK**.

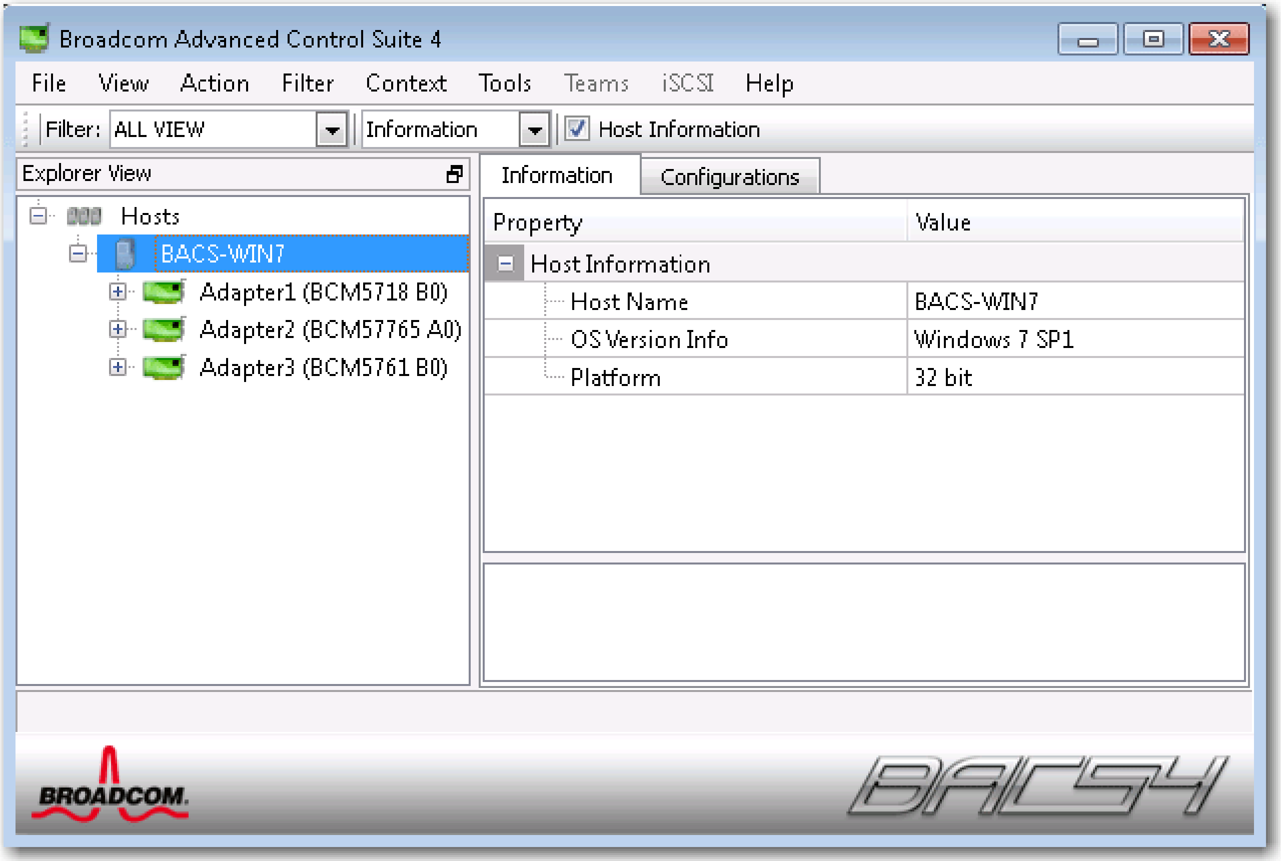
Managing the Host

At the host level, you can view host information and configure parameters from the following tabs:

- Information
- Configuration

To view host information

Select the host in the **Explorer View** pane, and then select the **Information** tab to view host-level information.



Property	Value
Host Information	
Host Name	BACS-WIN7
OS Version Info	Windows 7 SP1
Platform	32 bit

Information Tab: Host Information

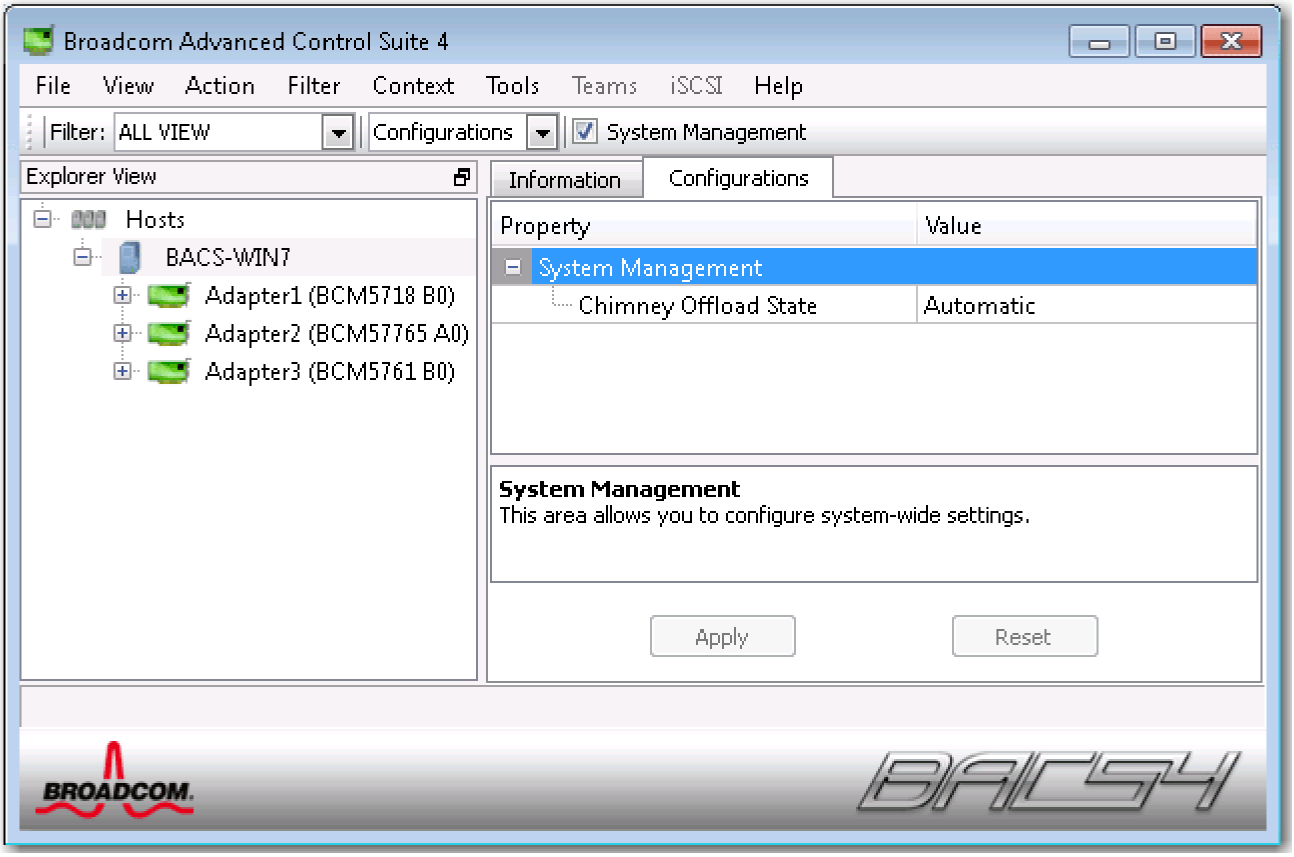
Host Name. Displays the name of the host.

OS Version Info. Displays the operating system, including the version.

Platform. Displays the hardware architecture platform (for example, 32-bit or 64-bit)

To configure the host

Select the host in the **Explorer View** pane, and then select the **Configuration** tab to configure host-level parameters.



Property	Value
System Management	
Chimney Offload State	Automatic

System Management
This area allows you to configure system-wide settings.

Configuration Tab: System Management

Chimney Offload State. Enable or disable chimney offload at the host level, rather than at the device level, and then click **Apply**.

MANAGING THE NETWORK ADAPTER

The installed network adapters appear one level below the host in the hierarchical tree in the Explorer View pane. At the adapter level, you can view information and configure parameters from the following tabs:

- Information
- Configuration

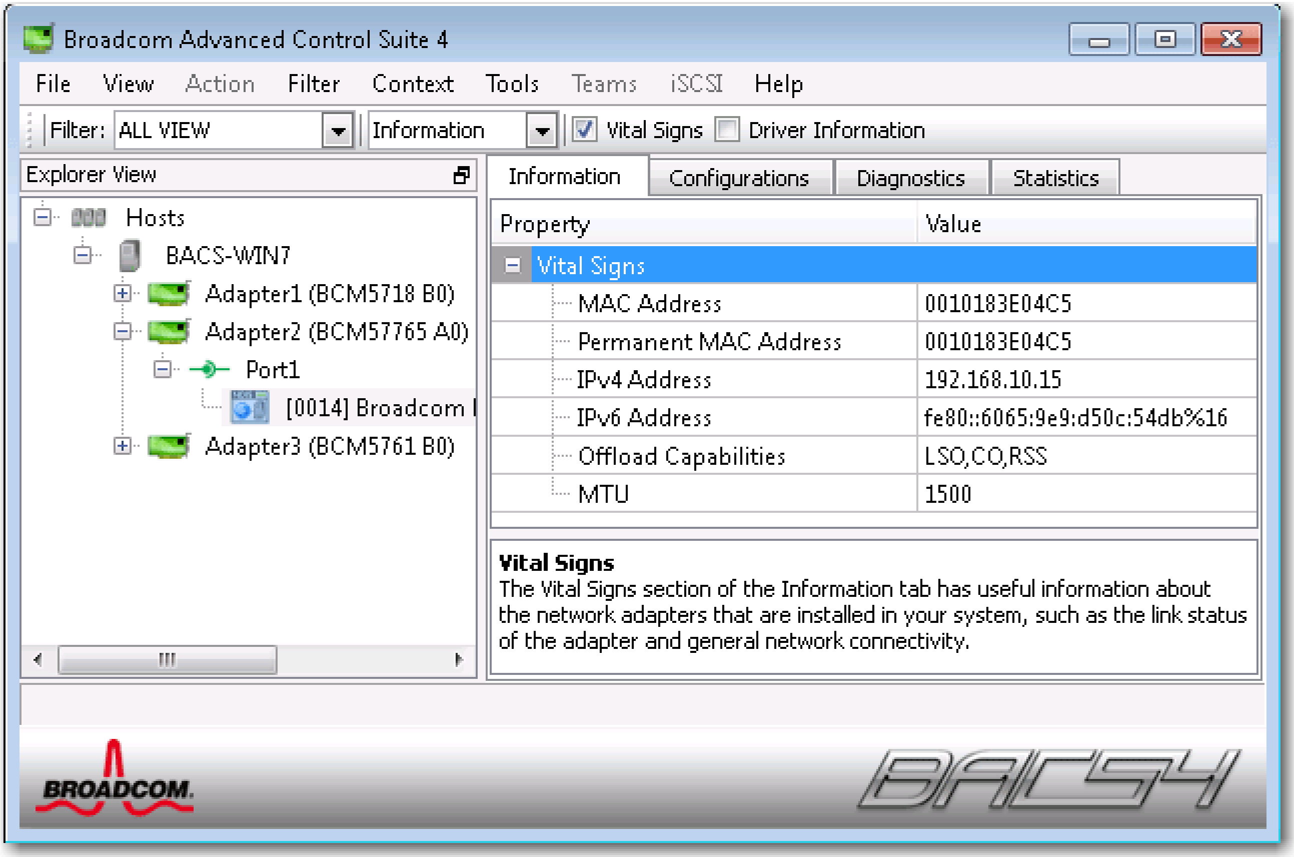
VIEWING ADAPTER INFORMATION

The **Vital Signs** section of the **Information** tab has useful information about the network adapters that are installed in your system, such as the link status of the adapter and general network connectivity.

Select the network adapter in the **Explorer View** pane, and then select the **Information** tab to view adapter-level information.

NOTES:

- Information about Broadcom network adapters may be more comprehensive than information about network adapters made by others.
- Some information may not be available for all Broadcom network adapters.



Property	Value
Vital Signs	
MAC Address	0010183E04C5
Permanent MAC Address	0010183E04C5
IPv4 Address	192.168.10.15
IPv6 Address	fe80::6065:9e9:d50c:54db%16
Offload Capabilities	LSO,CO,RSS
MTU	1500

Vital Signs
The Vital Signs section of the Information tab has useful information about the network adapters that are installed in your system, such as the link status of the adapter and general network connectivity.

MAC Address. A physical MAC (media access control) address that is assigned to the adapter by the manufacturer. The physical address is never all 0s.

Permanent MAC Address. The unique hardware address assigned to the network adapter.

IP Address. The network address associated with the adapter. If the IP address is all 0s, the associated driver has not been bound with Internet Protocol (IP).

Link Status. The status of the network link.

- **Up.** A link is established.
- **Down.** A link is not established.

Duplex. The adapter is operating in the indicated duplex mode.

Speed (in Mbps). The link speed of the adapter, in megabits per second.

Offload Capabilities. The offload capabilities supported by the adapter.

This information is only available for Broadcom NetXtreme adapters.

- **LSO**. Large Send Offload (LSO) prevents an upper level protocol such as TCP from breaking a large data packet into a series of smaller packets with headers appended to them.
- **CO.** Checksum Offload (CO) allows the TCP/IP/UDP checksums for send and receive traffic to be calculated by the adapter hardware rather than by the host CPU.

LiveLink IP Address. The network address of the LiveLink enabled adapter.

VIEWING DRIVER INFORMATION

The **Driver Information** section of the **Information** tab displays data about the driver for the selected network adapter.

To view Driver Information for any installed network adapter, click the name of the adapter listed in the Explorer View pane, then click the **Information** tab.

Driver Status. The status of the adapter driver.

- **Loaded**. Normal operating mode. The adapter driver has been loaded by Windows and is functioning.
- **Not Loaded**. The driver associated with the adapter has not been loaded by Windows.
- **Information Not Available**. The value is not obtainable from the driver that is associated with the adapter.

Driver Name. The file name of the adapter driver.

Driver Version. The current version of the adapter driver.

Driver Date. The creation date of the adapter driver.

VIEWING RESOURCE INFORMATION

The **Resources** section of the **Information** tab displays information about connections and other essential functions for the selected network adapter.

To view Resources for any installed network adapter, click the name of the adapter listed in the Explorer View pane, then click the **Information** tab.

Note: Some information may not be available for all Broadcom network adapters.

Bus Type. The type of input/output (I/O) interconnect used by the adapter.

Slot No. The slot number on the system board occupied by the adapter. This item is not available for PCI Express type adapters.

Bus Speed (MHz). The bus clock signal frequency used by the adapter. This item is not available for PCI Express type adapters.

Bus Width (bit). The number of bits that the bus can transfer at a single time to and from the adapter. This item is not available for PCI Express type adapters.

Bus No. Indicates the number of the bus where the adapter is installed.

Device No. The number assigned to the adapter by the operating system.

Function No. The port number of the adapter. For a single-port adapter, the function number is 0. For a two-port adapter, the function number for the first port is 0, and the function number for the second port is 1.

Interrupt Request. The interrupt line number that is associated with the adapter. Valid numbers range from 2 to 25.

Memory Address. The memory mapped address that is assigned to the adapter. This value can never be 0.

VIEWING HARDWARE INFORMATION

The Hardware section of the **Information tab** displays information about the hardware settings for the selected network adapter.

To view Hardware for any installed network adapter, click the name of the adapter listed in the Explorer View pane, then click the Information tab.

Note: Some information may not be available for all Broadcom network adapters.

ASIC Version. The chip version of the Broadcom adapter (this information is not available for adapters made by others).

Firmware Version. The firmware version of the Broadcom adapter (this information is not available for adapters made by others). This information is only available for Broadcom NetXtreme adapters.

Vendor ID. The vendor ID.

Device ID. The adapter ID.

Subsystem Vendor ID. The subsystem vendor ID.

Subsystem ID. The subsystem ID.

TESTING THE NETWORK

The **Network Test** option on the **Diagnostics** tab lets you verify IP network connectivity. This test verifies if the driver is installed correctly and tests connectivity to a gateway or other specified IP address on the same subnet.

The network test uses TCP/IP to send ICMP packets to remote systems, then waits for a response. If a gateway is configured, the test automatically sends packets to that system. If a gateway is not configured or if the gateway is unreachable, the test prompts for a destination IP address.

NOTES:

- The network test option is not available on adapters that are grouped into a team (see Configuring Teaming).
- This feature can be used with Windows Server managed hosts only. It is not available for hosts operating on Linux or other OSes. You can, however use BACS on a Linux client to connect to a Windows Server host and run the network test utility.

To run the network test using the BACS GUI

1. Click the name of the adapter to test in the Explorer View pane.
2. From the **Select a test to run** list, select **Network Test**.
3. To change the destination IP address, select **IP address to ping**, then click the browse button (…). In the Network Test window, enter a Destination IP address, then click **OK**.
4. Click **Run**.

The results of the network test are displayed in the **Status** field.

To run the network test using the BACS CLI

You can use the following CLI command to perform a network diagnostic test for the specified target. This command is available for NDIS and virtual adapters.

```
BACScli -t <target type> -f <target format> -i <target ID> networkdiag [-p <IP address>]
```

Examples:

1. The following command runs the network test for the current selected NDIS adapter.

   ```
   BACScli -t NDIS -f mac -i 0010181a1b1c "networkdiag -p 192.168.1.5"
   ```

2. The following command runs the network test for the current selected virtual adapter. Since there is no IP address specified, BACScli will use gateway address for the test.

   ```
   BACScli -t VNIC -f mac -i 0010181a1b1c "networkdiag"
   ```

In Interactive mode, use the `list <view>` and `select <idx>` commands to select the desired target device. Use `networkdiag [-p <IP address>]` to run the network diagnostics test for the selected target.

Examples:

1. The following command runs the network test for the currently selected NDIS adapter.

   ```
   networkdiag -p 192.168.1.5
   ```

2. The following command runs the network test for the current selected virtual adapter.

   ```
   networkdiag
   ```

RUNNING DIAGNOSTIC TESTS

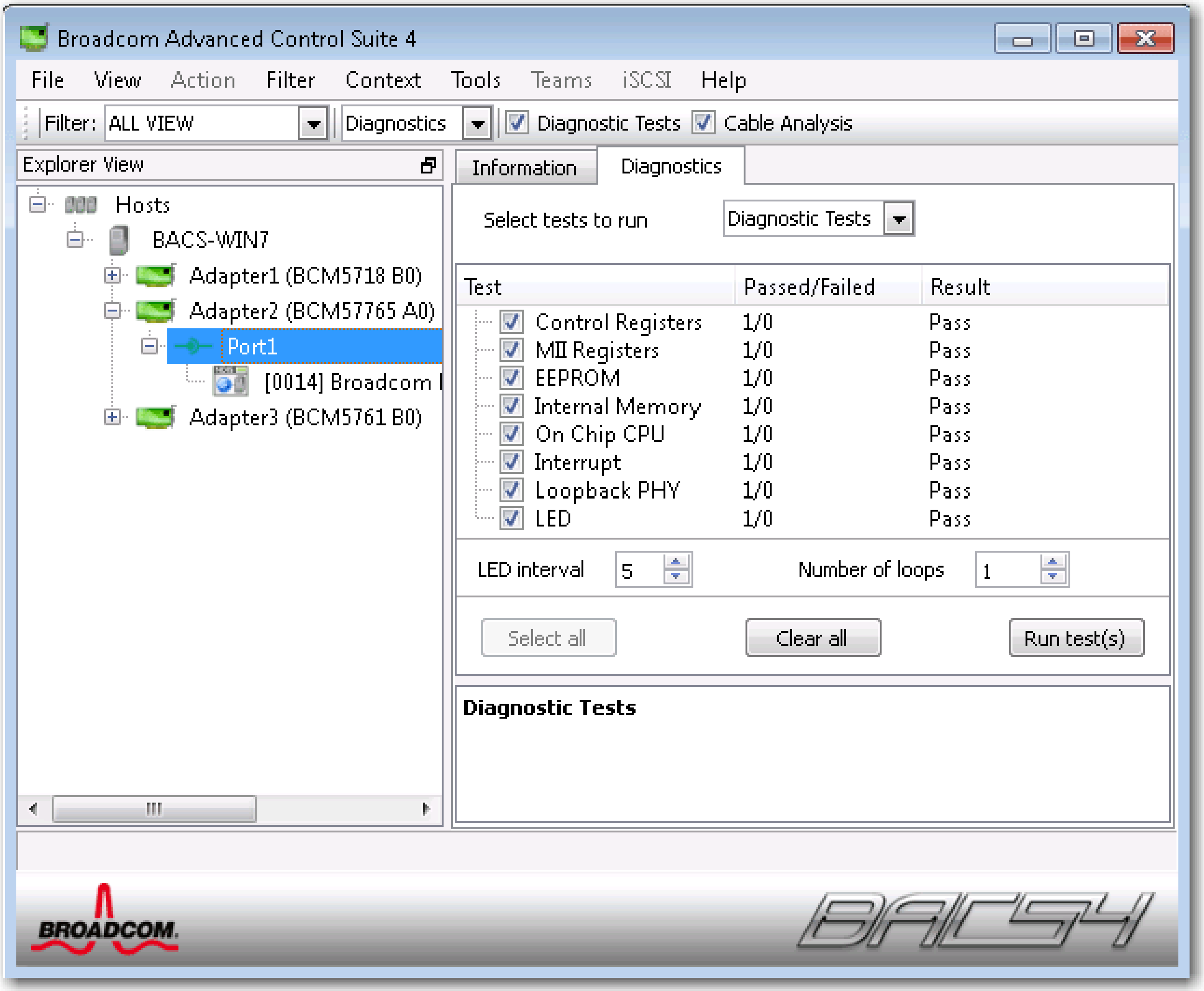
The **Diagnostic Tests** option on the **Diagnostics** tab lets you check the state of the physical components on a Broadcom network adapter. You can trigger the tests manually, or choose to have BACS 4 continuously perform them. If the test are performed continuously, then the number of passes and fails in the **Result** field for each test increments every time the tests are performed. For example, if a test is performed four times and there are no fails, the value in the **Result** field for that test is 4/0. However, if there were three passes and one fail, the value in the **Result** field is 3/1.

NOTES:

- This feature can be used with Windows Server managed hosts only. It is not available for hosts operating on Linux or other OSes. You can, however use BACS on a Linux client to connect to a Windows Server host and run the diagnostic test utility.
- You must have administrator privileges to run diagnostic tests.
- The network connection is temporarily lost while these tests are running.
- Not all Broadcom adapters support each test.

To run the diagnostic tests once using the BACS GUI

1. Click the name of the adapter to test in the Explorer View pane and select the Diagnostics tab.
2. From the **Select a test to run** list, select **Diagnostic Tests**.
3. Select the diagnostic tests you want to run. Click **Select All** to select all tests or **Clear All** to clear all test selections.
4. Select the number of times to run the tests from **Number of loops**.
5. Click **Run test(s)**.
6. In the error message window that warns of the network connection being temporarily interrupted, click **Yes**. The results are displayed in the **Result** field for each test.



Filter: ALL VIEW | Diagnostics | ☑ Diagnostic Tests ☑ Cable Analysis

Select tests to run: Diagnostic Tests

Test	Passed/Failed	Result
☑ Control Registers	1/0	Pass
☑ MII Registers	1/0	Pass
☑ EEPROM	1/0	Pass
☑ Internal Memory	1/0	Pass
☑ On Chip CPU	1/0	Pass
☑ Interrupt	1/0	Pass
☑ Loopback PHY	1/0	Pass
☑ LED	1/0	Pass

LED interval: 5

Number of loops: 1

Diagnostic Tests

Control Registers. This test verifies the read and write capabilities of the network adapter registers by writing various values to the registers and verifying the results. The adapter driver uses these registers to perform network functions such as sending and receiving information. A test failure indicates that the adapter may not be working properly.

MII Registers. This test verifies the read and write capabilities of the registers of the physical layer (PHY). The physical layer is used to control the electrical signals on the wire and to configure network speeds such as 1000 Mbit/s.

EEPROM. This test verifies the content of the electrically erasable programmable read-only memory (EEPROM) by reading a portion of the EEPROM and computing the checksum. The test fails if the computed checksum is different from the checksum stored in the EEPROM. An EEPROM image upgrade does not require a code change for this test.

Internal Memory. This test verifies that the internal memory of the adapter is functioning properly. The test writes patterned values to the memory and reads back the results. The test fails if an erroneous value is read back. The adapter cannot function if its internal memory is not functioning properly.

On-Chip CPU. This test verifies the operation of the internal CPUs in the adapter.

Interrupt. This test verifies that the Network Device Driver Interface Specification (NDIS) driver is able to receive interrupts from the adapter.

LoopBack MAC. This test verifies that the NDIS driver is able to send packets to and receive packets from the adapter.

LoopBack PHY. This test verifies that the NDIS driver is able to send packets to and receive packets from the adapter.

Test LED. This test causes all of the port LEDs to blink 5 times for the purpose of identifying the adapter.

To run the diagnostic tests using the BACS CLI

You can use the following CLI command to run diagnostics tests on a specified target. This command is available for physical device ports only:

```
BACScli -t <target type> -f <target format> -i <target ID> "diag {[-c REG ] [-c MII ] [-c
EEP] [-c MEM] [-c CPU] [-c INT] [-c MACLB ] [-c PHYLB] [-c LED] | [-c ALL]} [-l <cnt> ] [ -
v <LEDIntv> ]"
```

Examples:

1. The following command displays all the diagnostics tests available for the current selected target.

   ```
   BACScli -t PHYPORTS -f bdf -i 01:00.00 "diag"
   ```

2. The following command runs the MII and LED tests for the selected target:

   ```
   BACScli -t PHYPORTS -f bdf -i 01:00.00 "diag -c MII -c LED"
   ```

3. The following command runs all the tests five times with an LED test interval of 8 ms for the selected target:

   ```
   BACScli -t PHYPORTS -f bdf -i 01:00.00 "diag -c all -l 5 -v 8"
   ```

In Interactive mode, use the `list <view>` and `select <idx>` commands to select the desired target device. Use the following command to run diagnostic tests for the selected target:

```
diag {[-c REG ] [-c MII ] [-c EEP] [-c MEM] [-c CPU] [-c INT] [-c MACLB ] [-c PHYLB] [-c
LED] | [-c ALL]} [-l <cnt> ] [ -v <LEDIntv> ]
```

Examples:

1. The following command displays all the diagnostics tests available for the current selected target.

   ```
   diag
   ```

2. The following command runs the MII and LED test for the selected target.

   ```
   diag -c MII -c LED
   ```

3. The following command runs all the tests five times, with an LED test interval of 8 ms for the selected target.

   ```
   diag -c all -l 5 -v 8
   ```

ANALYZING CABLES

The **Cable Analysis option** on the **Diagnostics** tab lets you monitor the conditions of each wire pair in an Ethernet Category 5 cable connection within an Ethernet network. The analysis measures the cable quality and compares it against the IEEE 802.3ab specification for compliance.

NOTES:

- This feature can be used with Windows Server managed hosts only. It is not available for hosts operating on Linux or other OSes. You can, however use BACS on a Linux client to connect to a Windows Server host and run the cable analysis utility.
- You must have administrator privileges to run the cable analysis test.
- The network connection is temporarily lost during an analysis.
- For Broadcom NetXtreme adapters, the cable analysis test can only run for gigabit link-speed connections and when there is no connection.
- This option is not available for all Broadcom network adapters.

To run a cable analysis using the BACS GUI

1. Connect the cable to a port on a switch where the port is set to **Auto** and the Speed & Duplex driver settings are also set to **Auto**.
2. Click the name of the adapter to test in the Explorer View pane.
3. From the **Select a test to run** list, select **Cable Analysis**. If the **Cable Analysis** option is not available, then from the **Context View** tab on the right side of the window, select **Diagnostics** and then select **Cable Analysis**.
4. Click **Run**.
5. In the error message window that warns of the network connection being temporarily interrupted, click **Yes**.

Distance. The valid cable distance in meters (except when the Noise result is returned).

Status. This shows the type of link on this cable pair.

- **Good**. Good cable/PCB signal paths, but no gigabit link.
- **Crossed**. Pin short or crosstalk along two or more cable/PCB signal paths.
- **Open**. One or both pins are open for a twisted pair.
- **Short**. Two pins from the same twisted pair are shorted together.
- **Noise**. Persistent noise present (most likely caused by Forced 10/100).
- **GB Link**. Gigabit link is up and running.
- **N/A**. Algorithm failed to reach a conclusion.

Link. The link connection speed and duplex mode.

Status. The status after the test is run, either completed or failed.

There are several factors that could have an effect on the test results:

- **Link partner**. Various switch and hub manufacturers implement different PHYs. Some PHYs are not IEEE compliant.
- **Cable quality**. Category 3, 4, 5, and 6 may affect the test results.
- **Electrical interference**. The testing environment may affect the test results.

To run a cable analysis using BACS CLI

You can use the following CLI commands to run cable analysis for the specified target. This command is available for physical device ports only.

```
BACScli -t <target type> -f <target format> -i <target ID> cablediag
```

Example:

1. The following command runs the cable diagnostics test for the current selected target.

```
BACScli -t PHYPORTS -f bdf -i 01:00.00 "cablediag"
```

In Interactive mode, use the `list <view>` and `select <idx>` commands to select the desired target device. Use the `cablediag` command to run the cable analysis test for the selected target.

Example:

1. The following command runs the cable diagnostics test for the currently selected NDIS adapter.

```
cablediag
```

SETTING ADAPTER PROPERTIES

Advanced on the **Configurations** tab allow you to view and change the values of the available properties of the selected adapter. The potentially available properties and their respective settings are described below.

NOTES:

- You must have administrator privileges to change the values for a property.
- The list of available properties for your particular adapter may be different.
- Some properties may not be available for all Broadcom network adapters.

To set adapter properties

1. Click the name of the adapter in the Explorer View pane, and click the **Configurations** tab.
2. From the **Advanced** section, select the property you want to set.
3. To change the value of a property, select an item from the property's list or type a new value, as appropriate (selection options are different for different properties).
4. Click **Apply** to confirm the changes to all properties. Click **Reset** to return the properties to their original values.

802.1p QOS. Enables *quality of service*, which is an Institute of Electrical and Electronics Engineering (IEEE) specification that treats different types of network traffic diversely to ensure required levels or reliability and latency according to the type of traffic. This property is disabled by default. Unless the network infrastructure supports QoS, do not enable this property. Otherwise, problems may occur.

Flow Control. Enables or disables the receipt or transmission of PAUSE frames. PAUSE frames allow the network adapter and a switch to control the transmit rate. The side that is receiving the PAUSE frame momentarily stops transmitting.

- **Auto** (default). PAUSE frame receipt and transmission are optimized.
- **Disable**. PAUSE frame receipt and transmission are disabled.
- **Rx PAUSE**. PAUSE frame receipt is enabled.
- **Rx/Tx PAUSE**. PAUSE frame receipt and transmission are enabled.
- **Tx PAUSE**. PAUSE frame transmission is enabled.

Speed & Duplex. The Speed & Duplex property sets the connection speed and mode to that of the network. Note that Full-Duplex mode allows the adapter to transmit and receive network data simultaneously.

- **10 Mb Full**. Sets the speed at 10 Mbit/s and the mode to Full-Duplex.
- **10 Mb Half**. Sets the speed at 10 Mbit/s and the mode to Half-Duplex.
- **100 Mb Full**. Sets the speed at 100 Mbit/s and the mode to Full-Duplex.
- **100 Mb Half**. Sets the speed at 100 Mbit/s and the mode to Half-Duplex.
- **Auto** (default). Sets the speed and mode for optimum network connection (recommended).

NOTES:

- Auto is the recommended setting. This setting allows the network adapter to dynamically detect the line speed of the network. Whenever the network capability changes, the network adapter automatically detects and adjusts to the new line speed and duplex mode. A speed of 1 Gbit/s is enabled by selecting Auto, when that speed is supported.
- 1 Gb Full Auto must be attached to a link partner that is also capable of a 1 Gb connection. Since the connection is limited to a 1 Gb connection only, the Ethernet@Wirespeed feature will be disabled. If the link partner supports a 1 Gb connection only, the Wake on LAN feature may not work. Additionally, management traffic (IPMI or UMP) in the absence of an operating system may also be affected.
- 10 Mb Half and 100 Mb Half settings force the network adapter to connect to the network in Half-Duplex mode. Note that the network adapter may not function if the network is not configured to operate at the same mode.
- 10 Mb Full and 100 Mb Full settings force the network adapter to connect to the network in Full-Duplex mode. The network adapter may not function if the network is not configured to operate at the same mode.

Wake Up Capabilities. Enables the network adapter to wake up from a low-power mode when it receives a network wake-up frame. Two types of wake-up frames are possible: Magic Packet and Wake Up Frame.

This property is only available for Broadcom NetXtreme adapters.

- **Both** (default). Selects both Magic Packet and Wake Up Frame as wake-up frames.
- **Magic Packet**. Selects Magic Packet as the wake-up frame.
- **None**. Selects no wake-up frame.
- **Wake Up Frame**. Selects Wake Up Frame as the wake-up frame and allows the network adapter to wake the system when an event such as a ping or an Address Resolution Protocol (ARP) request is received. This option works in conjunction with the operating system power mode saving and does not work if the Power Save setting does not enable WOL.

Priority & VLAN. Allows enabling both the prioritization of network traffic and VLAN tagging. VLAN tagging only occurs when the VLAN ID setting is configured with a value other than 0 (zero).

- **Priority & VLAN Enabled (default)**. Allows for packet prioritization and VLAN tagging.
- **Priority & VLAN Disabled**. Prevents packet prioritization and VLAN tagging.
- **Priority Enabled**. Allows packet prioritization only.
- **VLAN Enabled**. Allows VLAN tagging only.

Note: If an intermediate driver is managing the network adapter for VLAN tagging, the **Priority & VLAN Disabled** and **Priority Enabled** settings should not be used. Use the **Priority & VLAN Enabled** setting and change the **VLAN ID** to 0 (zero).

VLAN ID. Enables VLAN tagging and configures the VLAN ID when **Priority & VLAN Enabled** is selected as the **Priority & VLAN** setting. The range for the VLAN ID is 1 to 4094 and must match the VLAN tag value on the connected switch. A value of 0 (default) in this field disables VLAN tagging.

Risk Assessment of VLAN Tagging through the NDIS Miniport Driver

Broadcom's NDIS 6.0 miniport driver provides the means to allow a system containing a Broadcom adapter to connect to a tagged VLAN. On Windows XP systems, this support was only provided through the use of an intermediate driver (e.g., Broadcom Advanced Server Program - BASP). Unlike BASP, however, the NDIS 6 driver's support for VLAN participation is only for a single VLAN ID.

Also unlike BASP, the NDIS 6.0 driver only provides VLAN tagging of the outbound packet, but does not provide filtering of incoming packets based on VLAN ID membership. This is the default behavior of all miniport drivers. While the lack of filtering packets based on VLAN membership may present a security issue, the following provides a risk assessment based on this driver limitation for an IPv4 network:

A properly configured network that has multiple VLANs should maintain separate IP segments for each VLAN. This is necessary since outbound traffic relies on the routing table to identify which adapter (virtual or physical) to pass traffic through and does not determine which adapter based on VLAN membership.

Since support for VLAN tagging on Broadcom's NDIS 6.0 driver is limited to transmit (Tx) traffic only, there is a risk of inbound traffic (Rx) from a different VLAN being passed up to the operating system. However, based on the premise of a properly configured network above, the IP segmentation and/or the switch VLAN configuration may provide additional filtration to limit the risk.

In a back-to-back connection scenario, two computers on the same IP segment may be able to communicate regardless of their VLAN configuration since no filtration of VLAN membership is occurring. However, this scenario assumes that the security may already be breached since this connection type is not typical in a VLAN environment.

If the risk above is not desirable and filtering of VLAN ID membership is required, then support through an intermediate driver would be necessary.

Configuring Out-of-Band (OOB) Management Settings

Overview

The OOB Management section of the Configurations tab is used to configure parameters for the out-of-band management port on Broadcom network adapters. OOB management enables management of networked computers and servers when their operating system is absent. This includes a networked system with an inactive or inoperable operating system, or in a low-power system sleep state. Using industry-standard remote management protocols, a remote management console can control and monitor client systems via a channel separate from the data channel. Broadcom's implementation of these management protocols for its network adapters is called TruManage™ technology. Capabilities of OOB management include alerting and remote control.

NOTES: OOB Management is not available on all Broadcom NetXtreme network adapters.

TruManage

TruManage is a Broadcom technology that integrates Distributed Management Task Force (DMTF) open manageability standards and the Intelligent Platform Management Interface (IPMI) and Data Center Manageability Interface (DCMI) standards. TruManage provides advanced power management features that enable enterprise-class PC, mobile, and server systems to be fully managed from a management console.

Note: TruManage is available only on Broadcom NetXtreme network adapters that support one or more of the following standards (refer to your adapter documentation for information whether any of these are supported on your adapter):

- Desktop and mobile Architecture for System Hardware (DASH, a DMTF standard)
- Systems Management Architecture for Server Hardware (SMASH, a DMTF standard)
- Alert Standard Format (ASF, a DMTF standard)
- Data Center Manageability Interface (DCMI)
- Intelligent Platform Management Interface (IPMI)

TruManage supports the following features:

ASF

- Standardized by DMTF Pre-OS Working Group
- Alerts via SNMP Platform Event Traps (PETs)
- Secure remote query and control of system power state (ASF 2.0)

DASH/SMASH

DASH is supported on adapters based on the BCM5761 and BCM5762. SMASH is supported on adapters based on the BCM5725 only. TruManage supports the following features for these standards:

- Standardized by DMTF Desktop and Mobile Working Group (DMWG)
- WS-Management / SOAP / XML
- DMTF CIM Profiles

  - Base Desktop and Mobile
  - Physical Asset
  - CPU
  - System Memory
  - Power Supply
  - Sensors
  - Fan
  - Ethernet
  - Record Log
  - Role Based Authorization
  - Simple Identity Management
  - Power State Management
  - Profile Registration
  - Indications
  - Text Console Redirection (Including Telnet and SSH)
  - Software Inventory
  - Software Update
  - OS Status
  - Opaque Management Data
  - BIOS Management
  - Boot Control
- Class A (HTTP) and Class B (HTTPS / TLS) Security
- IPv4 and IPv6 network communications with DNS and DHCP support

Standardized Next-generation Platform Internal Communications

- Standardized by DMTF Platform Management Components Intercommunications (PMCI) Working Group
- Platform Level Data Models (PLDM)
- Management Component Transport Protocol (MCTP) / SMBus

Web Browser (HTML GUI) Management Interface

- OEM-Customizable
- HTTP and HTTPS

IPMI/DCMI

IPMI and DCMI are supported on the BCM5725 controller only. TruManage supports the following features:

- Intelligent Baseboard Management Controller (BCM)
- Power Control and Management
- Server Monitoring
- Advanced Configuration and Power Interface (ACPI) state
- Serial Over LAN (SoL)
- Boot Control
- Sensors
- Asset Tags

Starting OOB Management

To start OOB Management, select **OOB Management** from the BACS Configurations tab.

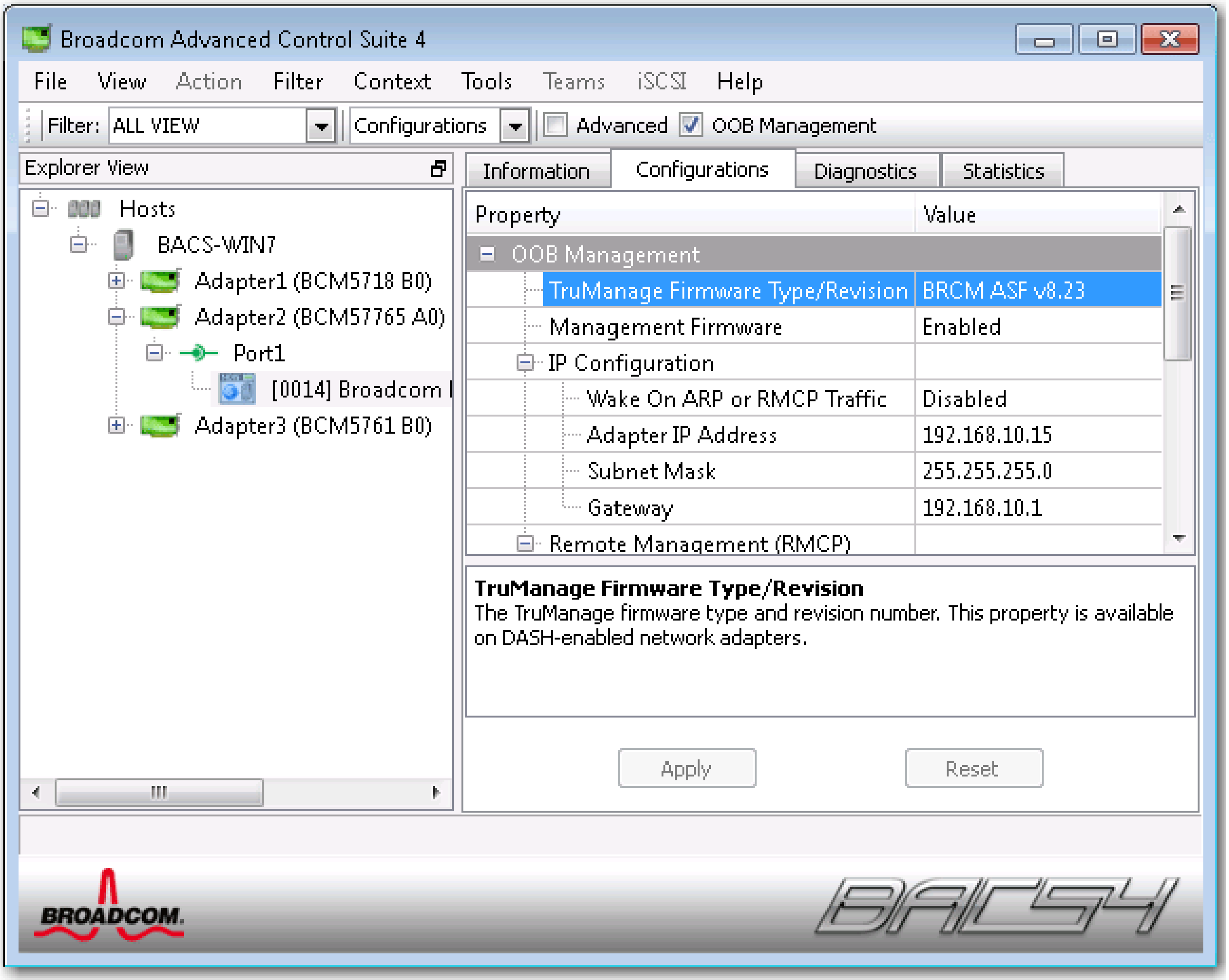
Configuring OOB Management Settings

To inspect or configure the basic OOB management operating parameters for a network adapter, select the TruManage-capable network adapter you want to configure, and then click **OOB Management** from the Configurations tab.

Note: Broadcom NetXtreme TruManage-enabled network adapters display **OOB Management** in the Configurations tab.

To configure general OOB management settings

1. Start BACS with elevated Admin privileges.
2. Click the name of the adapter in the Explorer View pane, and then click the **Configurations** tab.



Property	Value
OOB Management	
TruManage Firmware Type/Revision	BRCM ASF v8.23
Management Firmware	Enabled
IP Configuration	
Wake On ARP or RMCP Traffic	Disabled
Adapter IP Address	192.168.10.15
Subnet Mask	255.255.255.0
Gateway	192.168.10.1
Remote Management (RMCP)	

TruManage Firmware Type/Revision
The TruManage firmware type and revision number. This property is available on DASH-enabled network adapters.

3. From the **OOB Management** section, select the property you want to set.
4. To change the value of a property, select an item from the property's list or type a new value, as appropriate (selection options are different for different properties).

TruManage Firmware Type/Revision. The TruManage firmware type and revision number. This property is available only on network adapters that support TruManage.

Management Firmware. Enables the TruManage functionality in the selected network adapter. If there is more than one network adapter in your computer, be sure that you enable TruManage functionality in only one network adapter at a time.

Note: Enabling TruManage functionality in more than one network adapter in a system results in unpredictable behavior.

Wake on ARP or RMCP Traffic. Enables the network adapter to wake the computer upon receiving ARP or RMCP traffic while the computer is in low-power mode.

Note: The **Wake on ARP or RMCP Traffic** option is not available for TruManage-enabled network adapters.

Most Windows PCs today have the capability to conserve power by entering a low-power mode (stand-by, hibernate, or sleep). These computers also have the capability to wake up when an external event occurs. One such external event is when a network adapter receives an interesting packet. Typically, the computer wakes up if a network adapter receives one of the following types of interesting packets:

- Direct-IP
- Unicast
- NetBEUI name query

This Wake on LAN (WOL) behavior conflicts with the way a TruManage-enabled network adapter operates. When the computer enters low-power mode, a TruManage-enabled network adapter is still operational, sending PET messages and receiving and responding to RMCP messages and ARP requests. Received ARP and RMCP packets are direct-IP packets and would normally wake up the system, but this is not desirable behavior for most TruManage managed clients. By enabling or disabling wake on ARP or RMCP traffic, you can choose whether or not to wake-up the system when the network adapter receives an ARP or RMCP packet. When wake on TruManage traffic is enabled, the TruManage-enabled network adapter attempts to wake up the computer if the network adapter receives a TruManage power on/off frame.

Adapter IP Address. The adapter IP address of the network adapter is displayed next to the **Adapter IP Address**.

Subnet Mask. This value is the subnet mask that is applied to network addresses to determine the network segment to be used for routing considerations.

Default Gateway. The default gateway value is the network address of the gateway that will be used by the management firmware for packets destined for hosts external to the local network segment.

The displayed values are automatically updated whenever the network adapter IP address, subnet mask, or default gateway is changed via DHCP or manual configuration. The Broadcom Management Agent, which is a process that runs in the background as a service and has no user interface, automatically detects these changes and updates the properties in the ASF Configuration Table in the network adapter nonvolatile memory.

When the management console is located on a different subnet and is connected via a gateway router, the network adapter uses the subnet mask and default gateway values in the ASF Configuration Table to communicate with the management console.

IP Configuration. Use this section to configure the IP protocol and IP addresses.

Addressing Model. Identifies the IP addressing as either IPv4 Only, IPv6 Only, or IPv4 and IPv6.

IPV4. If IPv4 is the addressing model. Use this section to configure the IPv4 properties.

IPV6. If IPv6 is the addressing model, use this section to configure the IPv6 addresses.

Address. Enter the IP address. For IPv4, enter the IP address in dotted-decimal notation. For IPv6, enter the IP address using the following notation: X:X:X:X:X:X:X:X, where ‘X’ represents a hexadecimal number. When this parameter is set to 0.0.0.0, no IPv4 network communications will be supported by the management firmware. When this parameter is set to : :, only the IPv6 link-local address will be used for IPv6 network communications by the management firmware.

Subnet Mask. Enter the subnet mask value that is to be applied to the network addresses to determine the network segment to be used for routing considerations.

Gateway. Enter the gateway address.

Primary Name Server. Enter the IP address of the primary server that will be used by the management firmware for host name lookups via DNS. For IPv4, enter the IP address in dotted-decimal notation. For IPv6, enter the IP address using the following notation: X:X:X:X:X:X:X:X, where ‘X’ represents a hexadecimal number.

Secondary Name Server. Enter the IP address of the secondary server that will be used by the management firmware for host name lookups via DNS. For IPv4, enter the IP address in dotted-decimal notation. For IPv6, enter the IP address using the following notation: X:X:X:X:X:X:X:X, where ‘X’ represents a hexadecimal number.

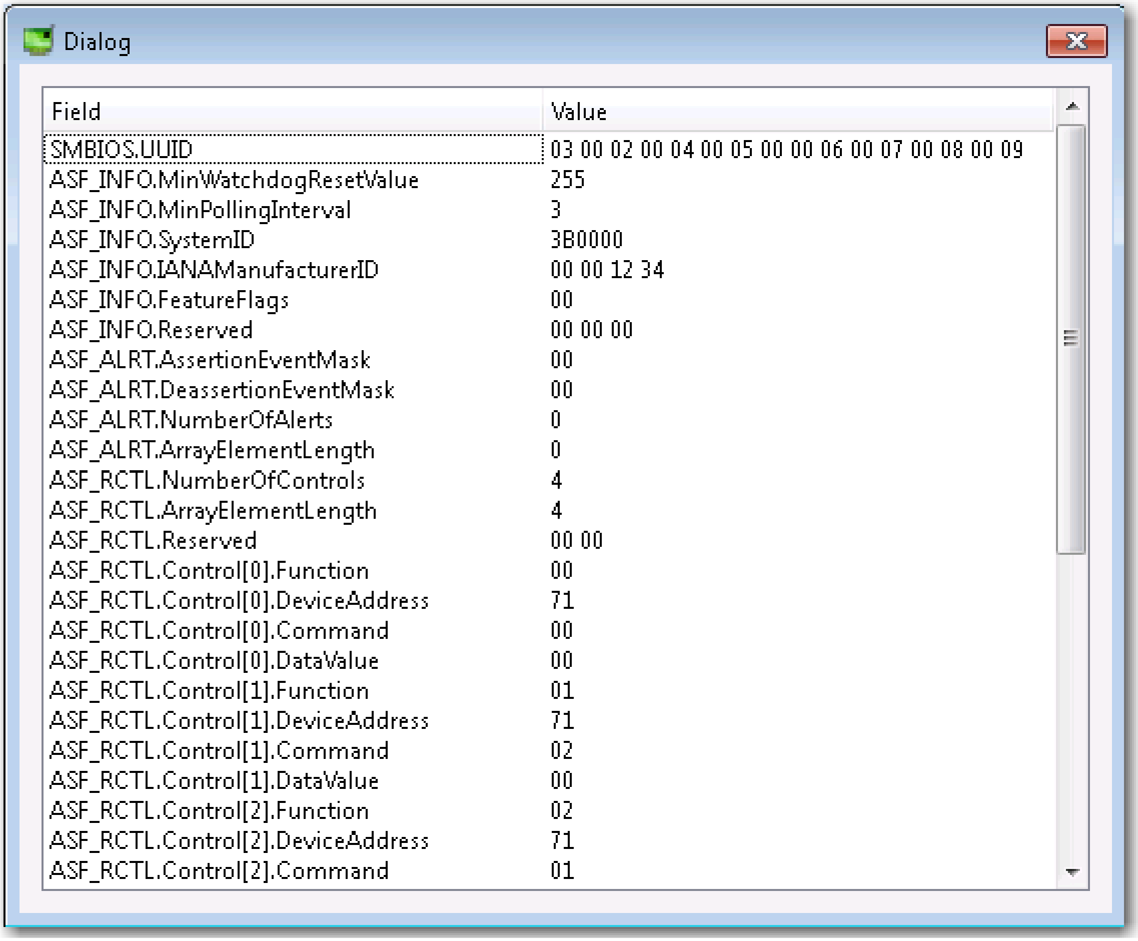
Dynamic Configuration (DHCP). Enables the use of a DHCP server when the host operating system network driver is not loaded. When this parameter is enabled and the operating system network driver is not loaded, the management firmware will perform DHCP network configuration negotiations and renewals.

IPV6. If IPv6 is the addressing model, use this section to configure the IPv6 addresses.

Subnet Prefix Length. Enter the subnet prefix length, in bits, for the IPv6 network address to determine the network segment to be used for IPv6 routing considerations. This value is typically 64 for IPv6. Do not use a forward slash with the subnet prefix length value.

System ASF! Description Table. The System ASF! Description Table defines the ASF-related capabilities and operating parameters of the computer, as defined by the computer manufacturer. This table is stored as an ACPI System Description Table in the computer firmware nonvolatile memory.

To view the System ASF! Description Table, click **Tools** from BACS and then select **View ASF!**.



Field	Value
SMBIOS.UUID	03 00 02 00 04 00 05 00 00 06 00 07 00 08 00 09
ASF_INFO.MinWatchdogResetValue	255
ASF_INFO.MinPollingInterval	3
ASF_INFO.SystemID	3B0000
ASF_INFO.IANAManufacturerID	00 00 12 34
ASF_INFO.FeatureFlags	00
ASF_INFO.Reserved	00 00 00
ASF_ALRT.AssertionEventMask	00
ASF_ALRT.DeassertionEventMask	00
ASF_ALRT.NumberOfAlerts	0
ASF_ALRT.ArrayElementLength	0
ASF_RCTL.NumberOfControls	4
ASF_RCTL.ArrayElementLength	4
ASF_RCTL.Reserved	00 00
ASF_RCTL.Control[0].Function	00
ASF_RCTL.Control[0].DeviceAddress	71
ASF_RCTL.Control[0].Command	00
ASF_RCTL.Control[0].DataValue	00
ASF_RCTL.Control[1].Function	01
ASF_RCTL.Control[1].DeviceAddress	71
ASF_RCTL.Control[1].Command	02
ASF_RCTL.Control[1].DataValue	00
ASF_RCTL.Control[2].Function	02
ASF_RCTL.Control[2].DeviceAddress	71
ASF_RCTL.Control[2].Command	01

CONFIGURING ALERTING

Alerting provides system health information and error notification in low-power and operating-system-absent states, as well as during normal operation to a remote management console. The parameters in the **Alerting** section of **OOB Management** are used to configure the settings related to SNMP platform event trap (PET) messages.

1. Click the name of the adapter in the Explorer View pane, and then click the **Configurations** tab.
2. From the **OOB Management** section, select the property you want to set.
3. To change the value of a property, select an item from the property's list or type a new value, as appropriate (selection options are different for different properties).

Transmit Platform Event Trap (PET) Messages. Enables the network adapter to transmit PET messages when this parameter is set to Enabled and the Destination Address parameter contains a valid IP address or host name. When this parameter is set to Disabled, PETs will not be transmitted and the remaining configuration parameters in this section will have no effect.

Transmit System Heartbeat Messages. When this paramter is set to Enabled and the Pet Heartbeat Interval parameter is non-zero, the management firmware will attempt to transmit periodic System Heartbeat PETs at the configured PET Heart Interval.

Management Console Address Type. Identify the addressing model of the management console.

Management Console Address. Type the IP address of the remote management console in the Management Console Address box to specify the IP address of the remote management console. An ASF or TruManage-enabled network adapter sends all PET messages to this IP address. The management console IP address is usually statically assigned and is seldom changed. If the management console IP address is changed, type the new IP address in the Management Console Address box.

Heartbeat Transmit Interval. Type the desired time interval in the **Heartbeat Transmit Interval** box to specify the time interval (in seconds) at which system heartbeat messages are sent.

SNMP Community Name. Type the desired community name in the **SNMP Community Name** box to specify the SNMP community name that is included in transmitted PET messages. The default SNMP community name is public.

PET Retransmission Interval. Type the desired time interval in the **PET Retransmission Interval** box to specify the time interval (in seconds) between retransmissions of a PET message. According to the ASF standard, each PET message (except the system heartbeat message) must be retransmitted three times to ensure successful delivery to the ASF management console. The default PET retransmission interval is 10 seconds.

CONFIGURING REMOTE MANAGEMENT CONTROL PROTOCOL (RMCP) MESSAGES

The remote management console can query an ASF or DASH-enabled client for capabilities and system presence or state information. On request, a client system will return the ASF feature set of the requested system. The properties in the **Remote Management (RMCP)** section are used to configure the settings related to secure remote management.

RMCP Support. Enables the management firmware to listen for incoming RMCP and/or Secure RMCP (RSP) requests based on the other parameters in this section. Note: With TruManage for servers, RMCP is used for discovery purposes only, whereas IPMI over LAN requests are sent using RMCP+.

A management console uses RMCP messages to communicate with an ASF or DASH managed client. When remote management is enabled, the network adapter acknowledges and responds to the following RMCP message types:

- Presence Ping
- Capabilities Request (not supported on TruManage for servers)
- System State Request (not supported on TruManage for servers)

If secure management is also enabled, the network adapter acknowledges and responds to the following secure RMCP message types:

- Open Session Request
- RAKP Message 1
- RAKP Message 3
- Close Session Request

If allowed by the remote control capabilities and security profile for the network adapter, the following operations can be performed remotely:

- Reset
- Power-up
- Power-down
- Power-reset

When remote management is disabled, the network adapter does not acknowledge or respond to RMCP messages.

RMCP Ping Only Support. Enables presence ping as the only RMCP method to test the connection between the DASH-enabled adapter and the management console. This option is not available in TruManage for servers.

RMCP Port Number. Enter the destination port in decimal notation. By default, the RMCP server communicates on port 623.

Secure RMCP Support (ASF 2.0). Enables the network adapter to receive and respond to secure Remote Management Control Protocol (RMCP) messages on UDP port 298h (664 decimal). This option is not available in TruManage for servers.

Secure RMCP Port Number. Enter the destination port in decimal notation. By default, the RMCP secure server communicates on port 624. This option is not available in TruManage for servers.

ASF 1.0 Compatibility. Enables the network adapter to receive and respond to insecure RMCP (ASF 1.0) messages on UDP port 26Fh (623 decimal). If Secure RMCP Support (ASF 2.0) is disabled, the network adapter automatically operates in ASF 1.0 compatibility mode, regardless of the setting for ASF 1.0 Compatibility. This option is not available in TruManage for servers.

Secure Session Timeout (seconds). To specify the amount of a time (in seconds) that a secure session must be inactive before it times out, type the desired timeout period in the Secure Session Timeout box. The network adapter supports a maximum of two simultaneous secure sessions, so it is important that inactive secure sessions time out after a reasonable period of time. The default secure session timeout period is 300 seconds (5 minutes). This option is not available in TruManage for servers.

Data Integrity Key. The value in the Data Integrity Key box is the shared secret key used for key generation operations (KG). Type the key in the Data Integrity Key box. If the generation key is in hexadecimal notation, select the (hex) check box. This option is not available in TruManage for servers.

Operator Authentication Keys. There are two types of authenticated user roles: Operator and Administrator. KO is the associated authentication key for Operator, and this parameter value is the 160-bit key used by the RSP Session Protocol (RSSP) when authenticating a remote management console requesting a secure RMCP session using the Operator role. Type the authentication key in the Authentication Key box. If the authentication key is in hexadecimal notation, select the (hex) check box. Possible values are 20 ASCII characters or 40 hexadecimal digits. This option is not available in TruManage for servers.

Administrator Authentication Keys. There are two types of authenticated user roles: Operator and Administrator. KA is the associated authentication key for Administrator, and this parameter value is the 160-bit key used by the RSP Session Protocol (RSSP) when authenticating a remote management console requesting a Secure RMCP session using the Administrator role. Type the authentication key in the Authentication Key box. If the authentication key is in hexadecimal notation, select the (hex) check box. Possible values include up to 20 ASCII characters or 40 hexadecimal digits. This option is not available in TruManage for servers.

> **Note:** Each security key (generation key, authentication key) may be typed as a set of up to 20 ASCII characters or as a set of hexadecimal bytes with each byte represented by 2 hexadecimal digits (0–F), with a maximum total length of 40 hexadecimal digits (20 bytes).

Both Operator and Administrator roles also have an associated set of rights that determines which RMCP Remote Control commands it has the right to execute on the managed client. These Remote Control commands include:

- Power-Up
- Reset
- Power-Reset
- Power-Down

To assign rights to an authenticated operator or administrator, select the appropriate check boxes in the **Rights** section.

CONFIGURING WEB SERVICES MANAGEMENT

Web Services (WS) Management is a DMTF specification that delivers standards-based web services management for DASH-enabled clients and SMASH-enabled servers. Both HTTP and HTTPS protocols are supported.

1. Click the name of the TruManage-enabled adapter in the Explorer View pane, and then click the **Configurations** tab.
2. From the **OOB Management** section, select the property you want to set.
3. To change the value of a property, select an item from the property's list or type a new value, as appropriate (selection options are different for different properties).

HTTP Support. This parameter determines whether or not HTTP communications will be supported by the management firmware. Both WS Management/HTTP (for DASH/SMASH Class A Security) and the web browser/GUI interface (over HTTP) depend on this parameter being set to Enabled.

HTTP Port Number. This parameter determines the TCP port number on which the management firmware will listen for incoming HTTP connections. This port will be used both for incoming WS Management/HTTP and web browser/GUI (over HTTP) requests.

HTTPS Support. This parameter determines whether or not HTTPS communications will be supported by the management firmware. Both WS Management/HTTPS (for DASH/SMASH Class B Security) and the web browser/GUI interface (over HTTPS) depend on this parameter being set to Enabled. HTTPS support also depends on the Private RSA Key and TLS Server Certificate records containing valid data.

HTTPS Port Number. Enter the destination port in decimal notation on which the management firmware will listen for incoming HTTPS connections. This port will be used both for incoming WS Management/HTTPS and web browser/GUI (over HTTPS) requests.

Using TruManage to Remotely Manage Systems

TruManage technology is Broadcom's solution for remotely managing and controlling mobile and desktop clients and servers from a management console. It enables remote and secure PC manageability in organizations with limited resources by eliminating desk-side visits, optimizing PC deployment, and enabling efficient platform provisioning regardless of the state of the system or operating system.

The managed system can be managed in-band or out-of-band.

- In-band: A management system sends management traffic through the managed system's network controller to the OS service, such as CIM. Management is accomplished through the management agent running on the OS on the managed system.
- Out of band: A management system sends management traffic to the managed system's network controller. The network controller runs the service that enables management independently of the managed system's host processor and OS.

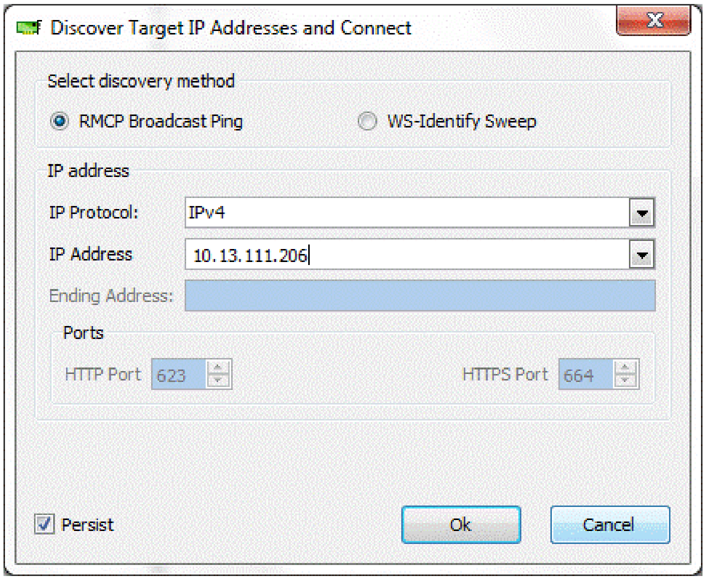
TruManage manages remote systems with a Broadcom NetXtreme TruManage-enabled adapter. This section assumes that the managed systems have been provisioned by the mobile/desktop client or server manufacturer.

Prior to managing a remote system, you must first add or discover the system and then connect to the system from a management console.

Discovering a Managed System

To discover a DASH- or SMASH-enabled Broadcom adapter for management via TruManage

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. From the **TruManage** menu, select **Discover TruManage Targets**. The **Discover Target IP Addresses and Connect** window appears.



Discover Target IP Addresses and Connect

Select discovery method

● RMCP Broadcast Ping ○ WS-Identify Sweep

IP address

IP Protocol: IPv4

IP Address 10.13.111.206

Ending Address:

Ports

HTTP Port 623 HTTPS Port 664

☑ Persist

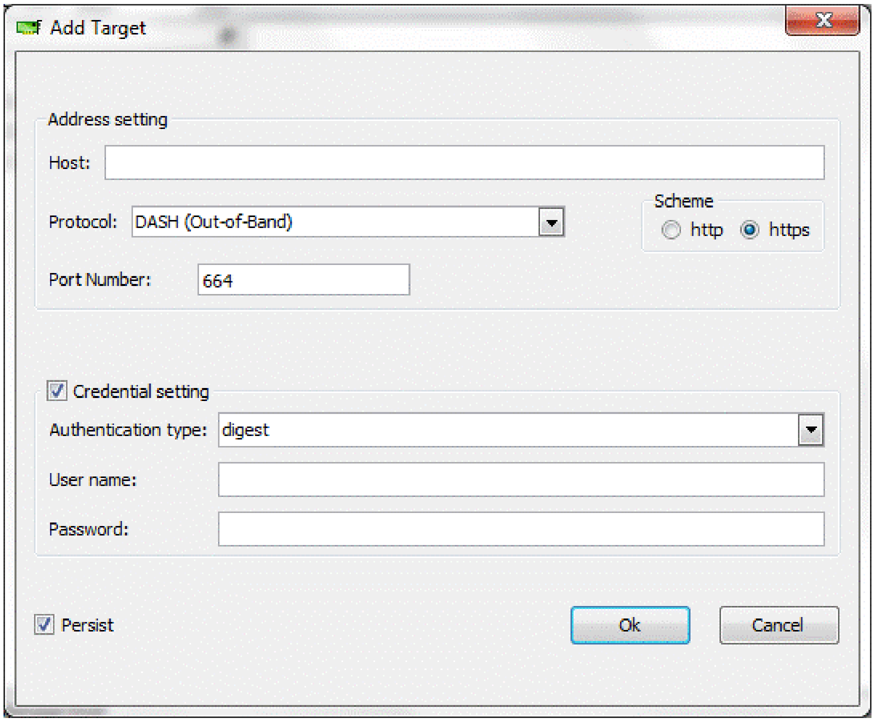
3. Select either **RMCP Broadcast Ping** or **WS-Identify Sweep** as the discovery method.

4. Select the **IP Protocol**.
5. Type the **IP Address** of the managed system and click **Ok**.

Adding a Managed System (Mobile or Desktop Computer)

To add a desktop or mobile computer with a DASH-enabled Broadcom adapter to be managed out of band via TruManage

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. From the **TruManage** menu, select **Add TruManage Target.** The **Add Target** window appears.



Add Target

Address setting

Host:

Protocol: DASH (Out-of-Band)

Scheme ○ http ● https

Port Number: 664

☑ Credential setting

Authentication type: digest

User name:

Password:

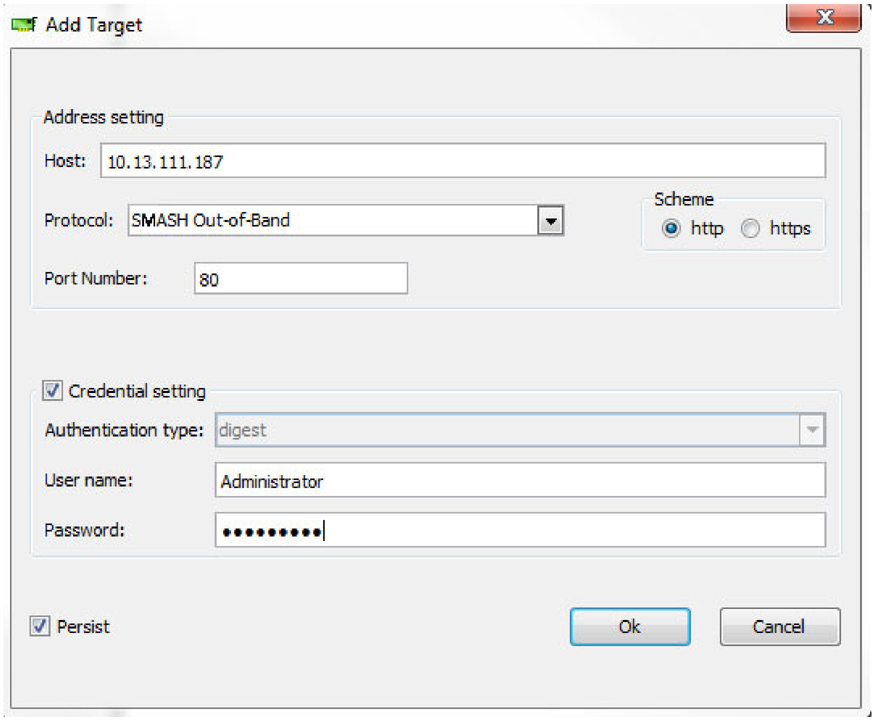
☑ Persist

3. Select For **Host**, type the managed system’s IP address.
4. For the **Protocol**, select **DASH (Out-of-Band)**.
5. For the **Scheme**, select **http** or **https**. The **Port Number** is 623 for HTTP and 664 for HTTPS.
6. Enter the **User name** and **Password** and click **Ok**.

Adding a Managed System (Server)

To add a server with a SMASH-enabled Broadcom adapter to be managed out of band via TruManage

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. From the **TruManage** menu, select **Add TruManage Target.** The **Add Target** window appears.



Host: 10.13.111.187

Protocol: SMASH Out-of-Band

Scheme: ● http ○ https

Port Number: 80

☑ Credential setting

Authentication type: digest

User name: Administrator

Password: •••••••••

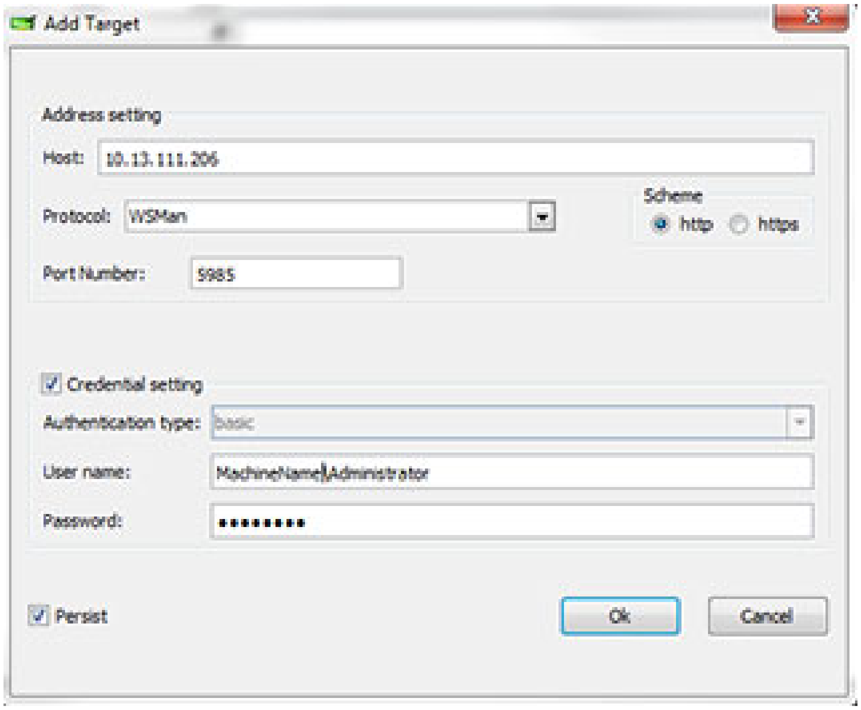
☑ Persist

3. For **Host**, type the managed system's IP address.
4. For the **Protocol**, select **Smash (Out-of-Band)**.
5. For the **Scheme**, select **http** or **https**. The **Port Number** is 80 for HTTP and 443 for HTTPS.
6. Enter the **User name** and **Password** and click **Ok**.

MAKING AN IN BAND CONNECTION TO A MANAGED SYSTEM

To connect to a managed system using an in band connection

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. From the **TruManage** menu, select **Connect TruManage Target**. The **Add Target** window appears.



Address setting

Host: 10.13.111.206

Protocol: WSMan

Scheme: ● http ○ https

Port Number: 5985

☑ Credential setting

Authentication type: basic

User name: MachineName\Administrator

Password: •••••••••

☑ Persist

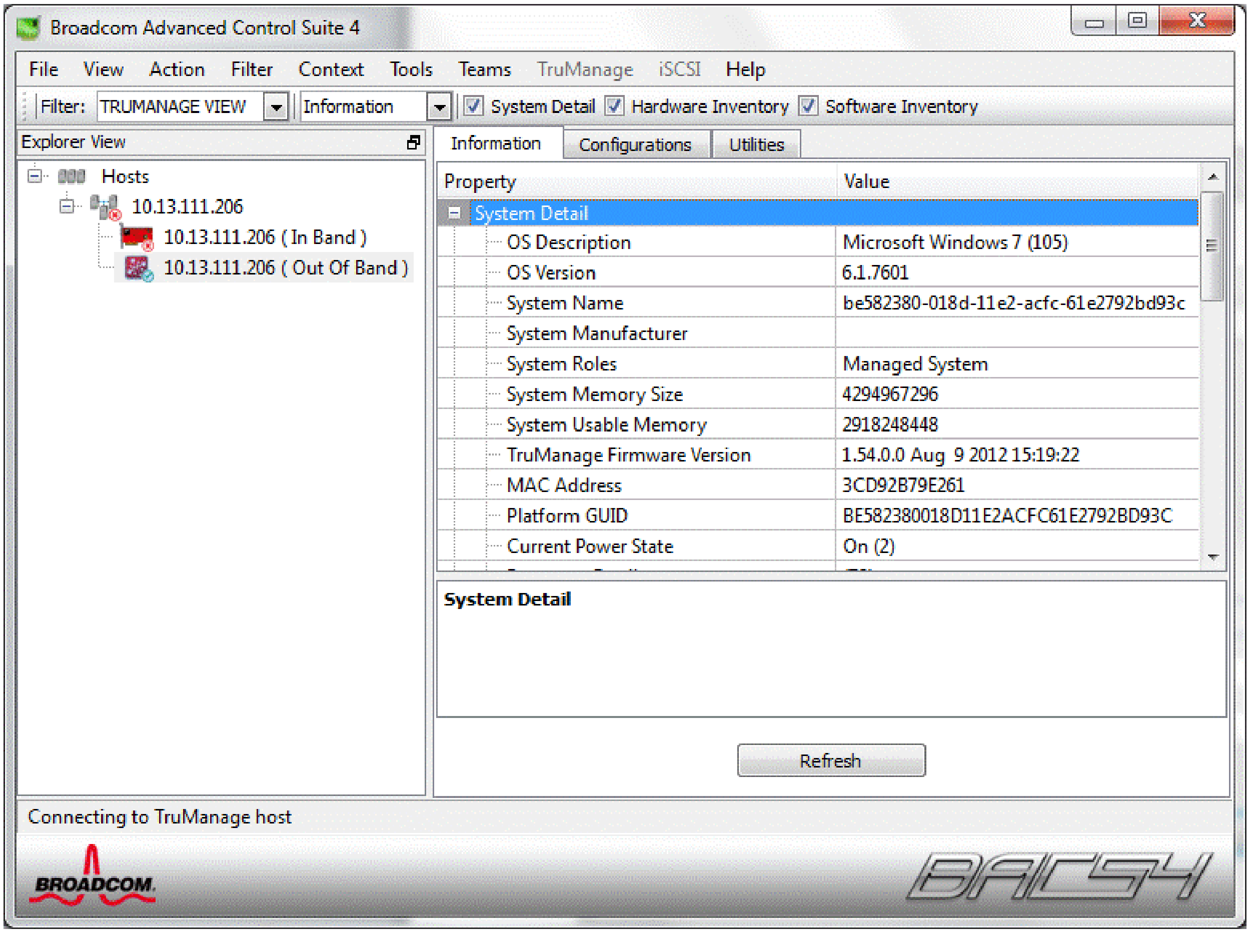
3. Select the **Protocol** and **Scheme**. Ensure that for HTTP, the **Port Number** is 5985 and for HTTPS, it is 5986.
4. Enter the **User name**. The user name is the managed system's Administrator user name because the connection is in band.
5. Type the **Password** and click **Ok**. The password is the managed system's password because the connection is in band.

Viewing System Information

TruManage technology enables comprehensive asset tracking of hardware and software inventory, including detailed information about the processor(s)/cache(s), system memory, chassis, fan(s), power supplies, and driver/firmware versions.

To view system information

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Information** tab.
3. Filter the view by selecting **System Detail**.


Broadcom Advanced Control Suite 4
File View Action Filter Context Tools Teams TruManage iSCSI Help
Explorer View
Hosts
10.13.111.206
10.13.111.206 (In Band)
10.13.111.206 (Out Of Band)
Information Configurations Utilities
Refresh
BROADCOM.
BACS4

Filter: TRUMANAGE VIEW | Information | ☑ System Detail ☑ Hardware Inventory ☑ Software Inventory

Property	Value
System Detail	
OS Description	Microsoft Windows 7 (105)
OS Version	6.1.7601
System Name	be582380-018d-11e2-acfc-61e2792bd93c
System Manufacturer	
System Roles	Managed System
System Memory Size	4294967296
System Usable Memory	2918248448
TruManage Firmware Version	1.54.0.0 Aug 9 2012 15:19:22
MAC Address	3CD92B79E261
Platform GUID	BE582380018D11E2ACFC61E2792BD93C
Current Power State	On (2)

System Detail

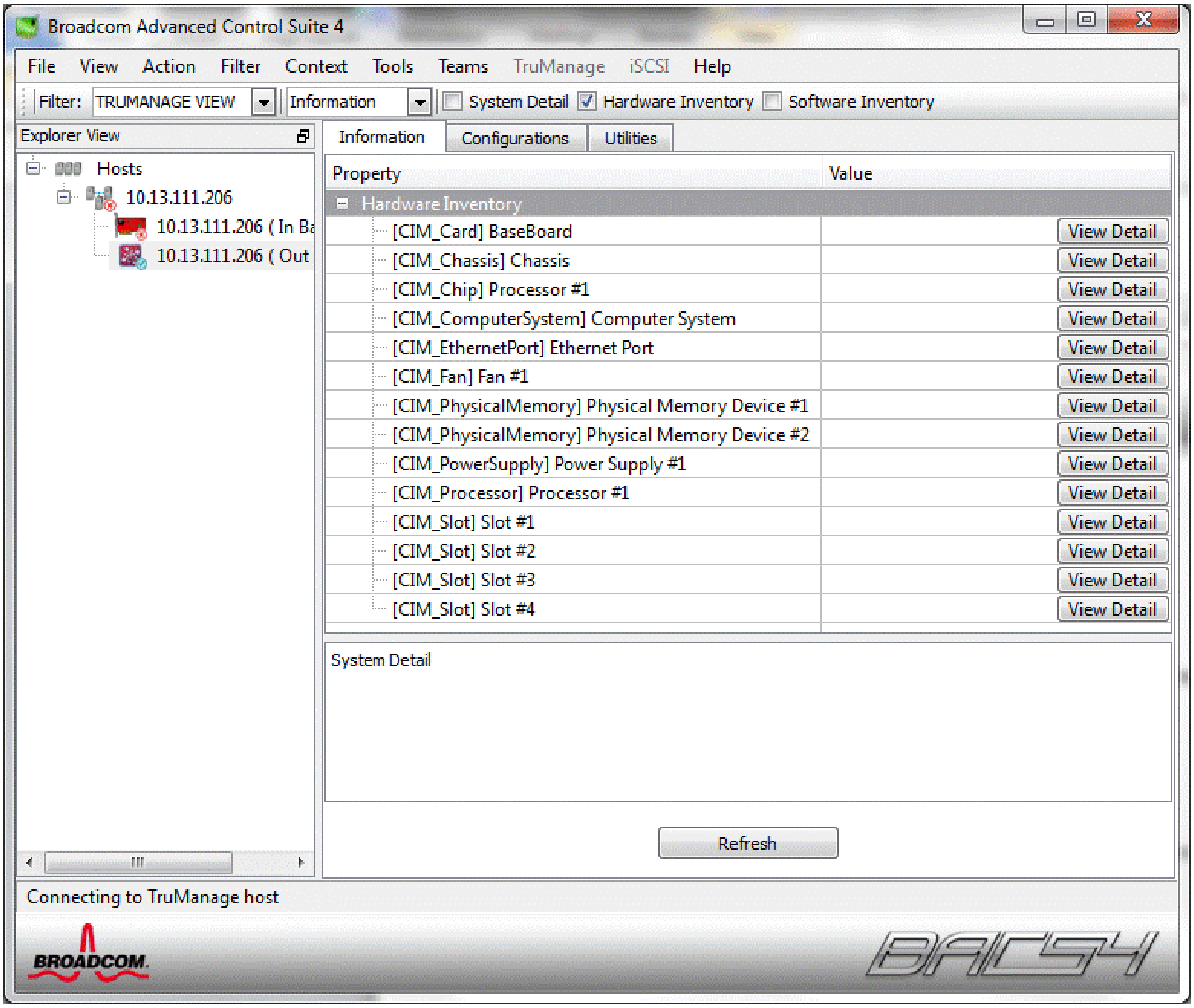
Connecting to TruManage host

VIEWING HARDWARE INVENTORY

Hardware inventory of the managed system is available from the **Information** tab. The available components from the **Hardware Inventory** section of the **Information** tab varies from system to system.

To view hardware inventory

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Information** tab.
3. Filter the view by selecting **Hardware Inventory**.

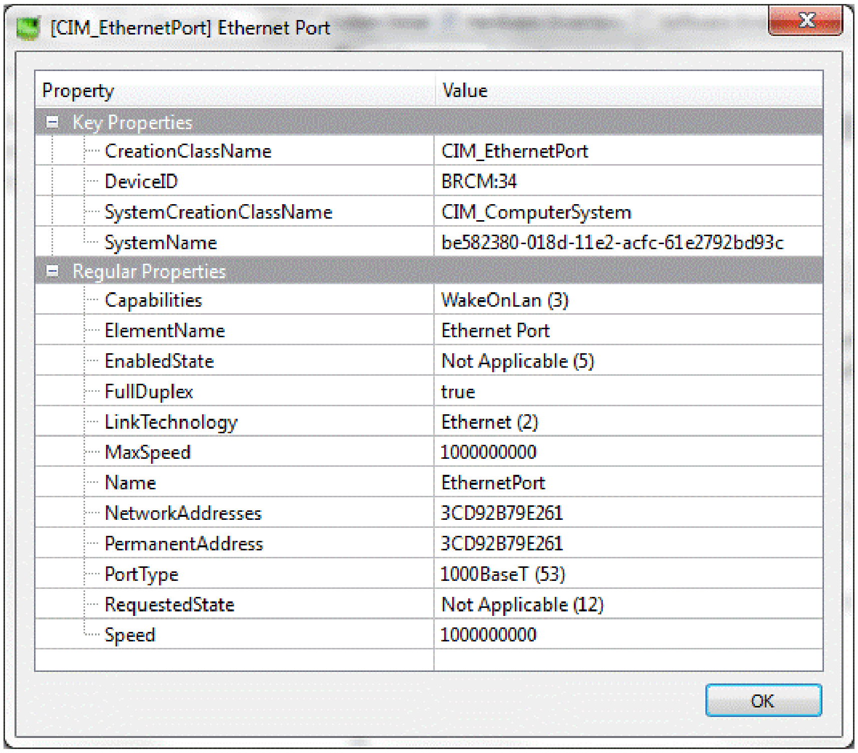


Filter: TRUMANAGE VIEW | Information | □ System Detail ☑ Hardware Inventory □ Software Inventory

Property	Value
⊟ Hardware Inventory	
[CIM_Card] BaseBoard	View Detail
[CIM_Chassis] Chassis	View Detail
[CIM_Chip] Processor #1	View Detail
[CIM_ComputerSystem] Computer System	View Detail
[CIM_EthernetPort] Ethernet Port	View Detail
[CIM_Fan] Fan #1	View Detail
[CIM_PhysicalMemory] Physical Memory Device #1	View Detail
[CIM_PhysicalMemory] Physical Memory Device #2	View Detail
[CIM_PowerSupply] Power Supply #1	View Detail
[CIM_Processor] Processor #1	View Detail
[CIM_Slot] Slot #1	View Detail
[CIM_Slot] Slot #2	View Detail
[CIM_Slot] Slot #3	View Detail
[CIM_Slot] Slot #4	View Detail

Connecting to TruManage host

4. To obtain the details of a particular hardware component, select **View Detail** to the right of the component. An example of the details for the Ethernet port is shown below.



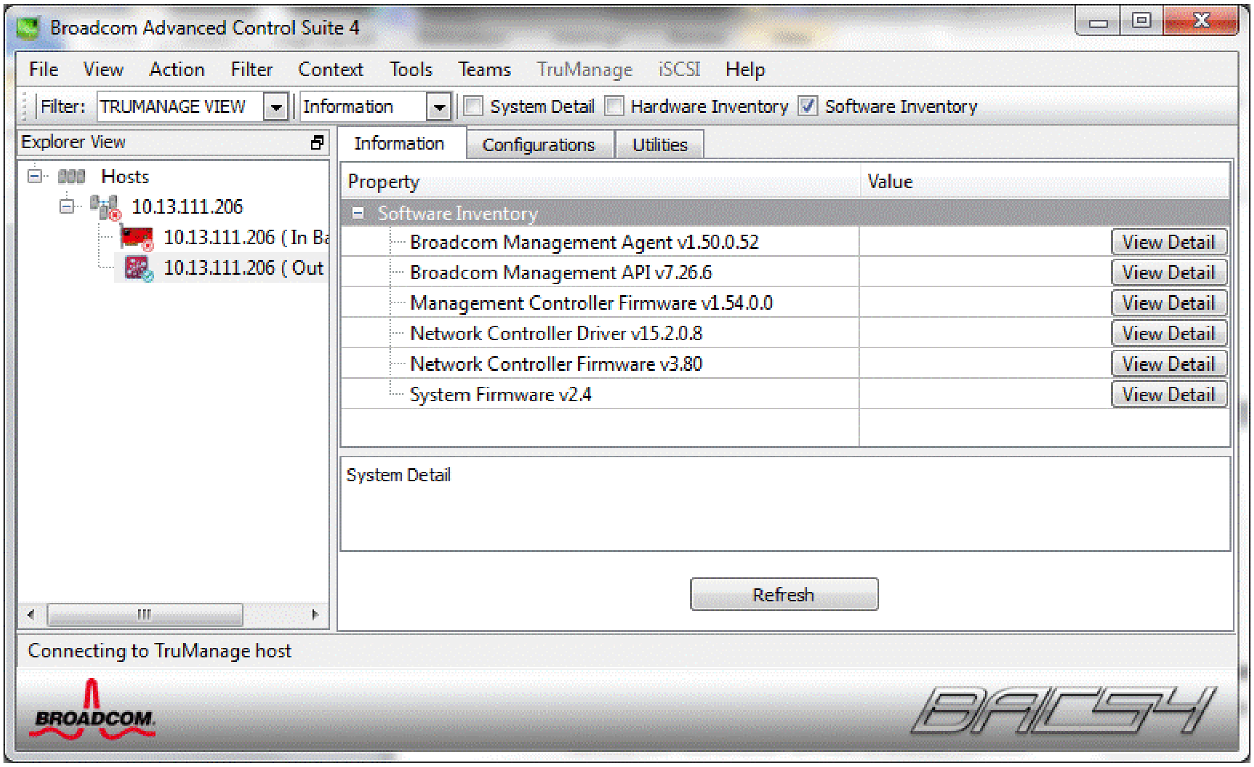
Property	Value
Key Properties	
CreationClassName	CIM_EthernetPort
DeviceID	BRCM:34
SystemCreationClassName	CIM_ComputerSystem
SystemName	be582380-018d-11e2-acfc-61e2792bd93c
Regular Properties	
Capabilities	WakeOnLan (3)
ElementName	Ethernet Port
EnabledState	Not Applicable (5)
FullDuplex	true
LinkTechnology	Ethernet (2)
MaxSpeed	1000000000
Name	EthernetPort
NetworkAddresses	3CD92B79E261
PermanentAddress	3CD92B79E261
PortType	1000BaseT (53)
RequestedState	Not Applicable (12)
Speed	1000000000

VIEWING SOFTWARE INVENTORY

Software inventory of the managed system is available from the **Information** tab.

To view hardware inventory

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Information** tab.
3. Filter the view by selecting **Software Inventory**.



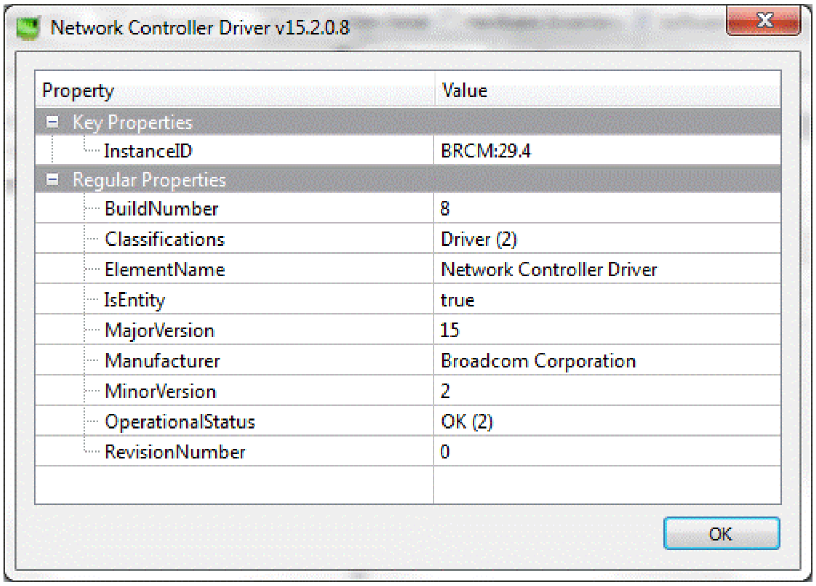
Filter: TRUMANAGE VIEW | Information | □ System Detail □ Hardware Inventory ☑ Software Inventory

Property	Value
⊟ Software Inventory	
Broadcom Management Agent v1.50.0.52	View Detail
Broadcom Management API v7.26.6	View Detail
Management Controller Firmware v1.54.0.0	View Detail
Network Controller Driver v15.2.0.8	View Detail
Network Controller Firmware v3.80	View Detail
System Firmware v2.4	View Detail

System Detail

Connecting to TruManage host

4. To obtain the details of a particular software component, select **View Detail** to the right of the component. An example of the details for the Network Controller Driver is shown below.



Network Controller Driver v15.2.0.8

Property	Value
⊟ Key Properties	
InstanceID	BRCM:29.4
⊟ Regular Properties	
BuildNumber	8
Classifications	Driver (2)
ElementName	Network Controller Driver
IsEntity	true
MajorVersion	15
Manufacturer	Broadcom Corporation
MinorVersion	2
OperationalStatus	OK (2)
RevisionNumber	0

Managing User Accounts

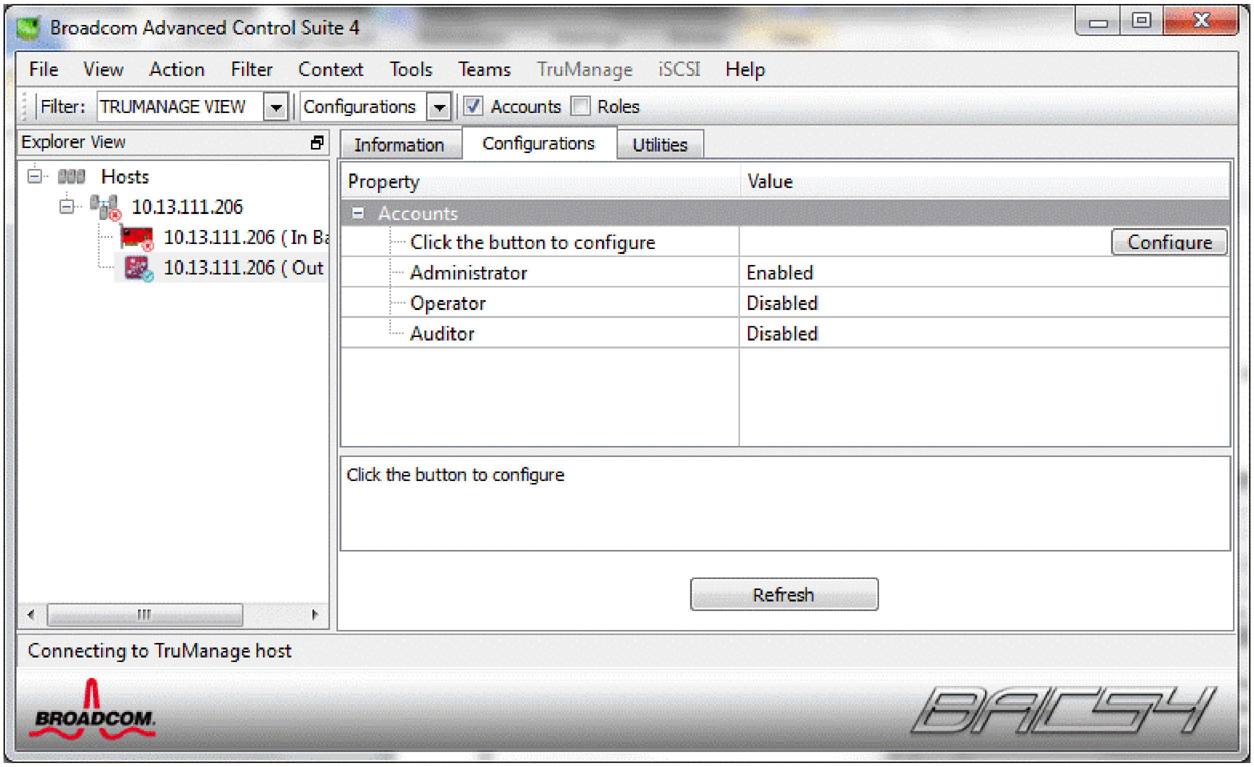
Note: These user accounts cannot be used for authenticating with ASF Secure RMCP/RSP or IPMI over LAN/ RMCP+.

User account management allows the system to efficiently and securely manage distinct platform management tasks assigned to various IT personnel. TruManage technology enables assigned IT managers to be associated with different roles, and each role can be configured to perform different OOB management functions. Supported roles can be dynamically configured. TruManage supports the following aspects of account management:

- Creating and deleting an account.
- Changing the enabled state of an account.
- Modifying the user name, organization name, and password of an account.
- Associating an account (identity) with specific roles tied to specific privileges.

To manage user accounts

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Configurations** tab.
3. Filter the view by selecting **Accounts**.



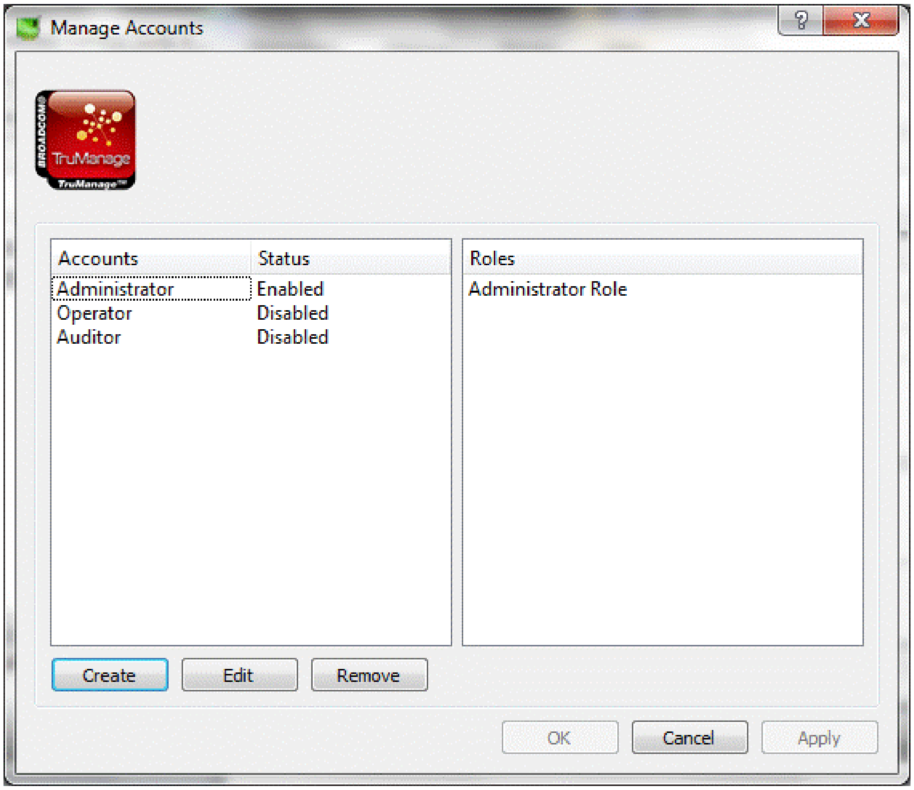
Filter: TRUMANAGE VIEW | Configurations | ☑ Accounts □ Roles

Property	Value
⊟ Accounts	
Click the button to configure	Configure
Administrator	Enabled
Operator	Disabled
Auditor	Disabled

Click the button to configure

Connecting to TruManage host

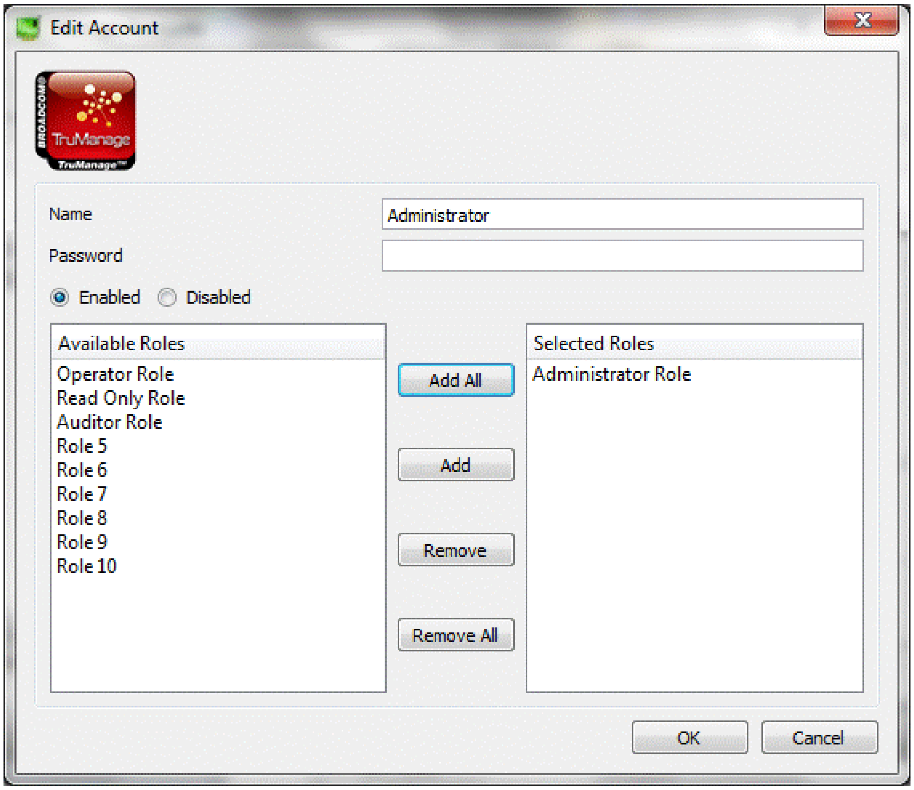
4. Select **Configure** to manage the accounts. The **Manage Accounts** window appears.



Accounts	Status
Administrator	Enabled
Operator	Disabled
Auditor	Disabled

Roles
Administrator Role

5. Create, edit, or remove an account. To edit an account, select **Edit**. The **Edit Accounts** window appears. You can select a role from the Available Roles list and click **Add** to move them to the Selected Roles list, or click **Add All**. You can select a role in the Selected Roles list and click **Remove** to remove it from the list, or you can click **Remove All** to remove all from the list.



Edit Account

Name: Administrator

Password:

● Enabled ○ Disabled

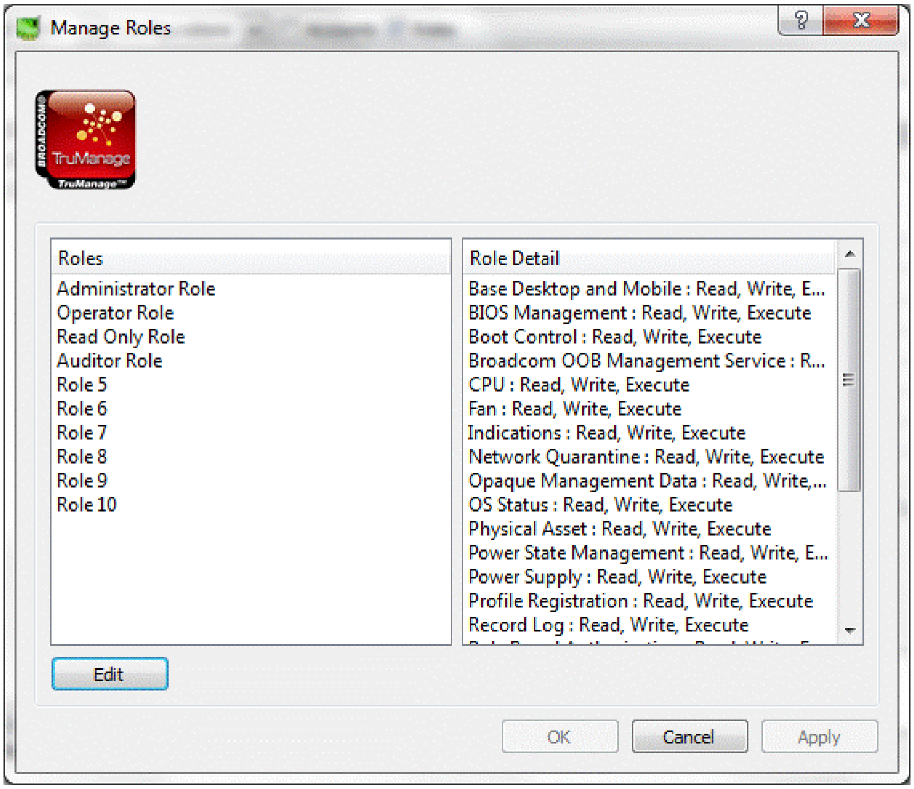
Available Roles	Selected Roles
Operator Role	Administrator Role
Read Only Role	
Auditor Role	
Role 5	
Role 6	
Role 7	
Role 8	
Role 9	
Role 10	

MANAGING ROLES

Each role can be configured to perform different management functions.

To manage roles

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Configurations** tab.
3. Filter the view by selecting **Roles**.
4. Select **Configure** to manage roles. The **Manage Roles** window appears.



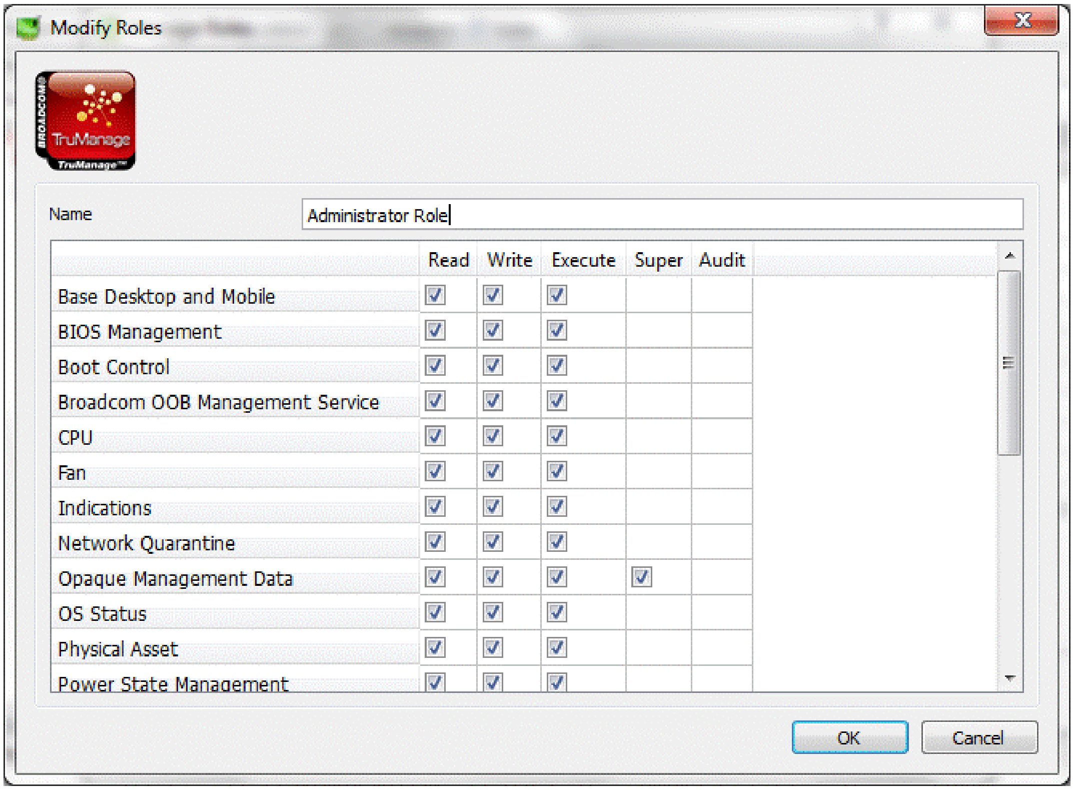
Roles

Administrator Role
Operator Role
Read Only Role
Auditor Role
Role 5
Role 6
Role 7
Role 8
Role 9
Role 10

Role Detail

Base Desktop and Mobile : Read, Write, E...
BIOS Management : Read, Write, Execute
Boot Control : Read, Write, Execute
Broadcom OOB Management Service : R...
CPU : Read, Write, Execute
Fan : Read, Write, Execute
Indications : Read, Write, Execute
Network Quarantine : Read, Write, Execute
Opaque Management Data : Read, Write,...
OS Status : Read, Write, Execute
Physical Asset : Read, Write, Execute
Power State Management : Read, Write, E...
Power Supply : Read, Write, Execute
Profile Registration : Read, Write, Execute
Record Log : Read, Write, Execute

5. Select **Edit** to change the capabilities of the roles. The **Modify Roles** window appears.



Name: Administrator Role

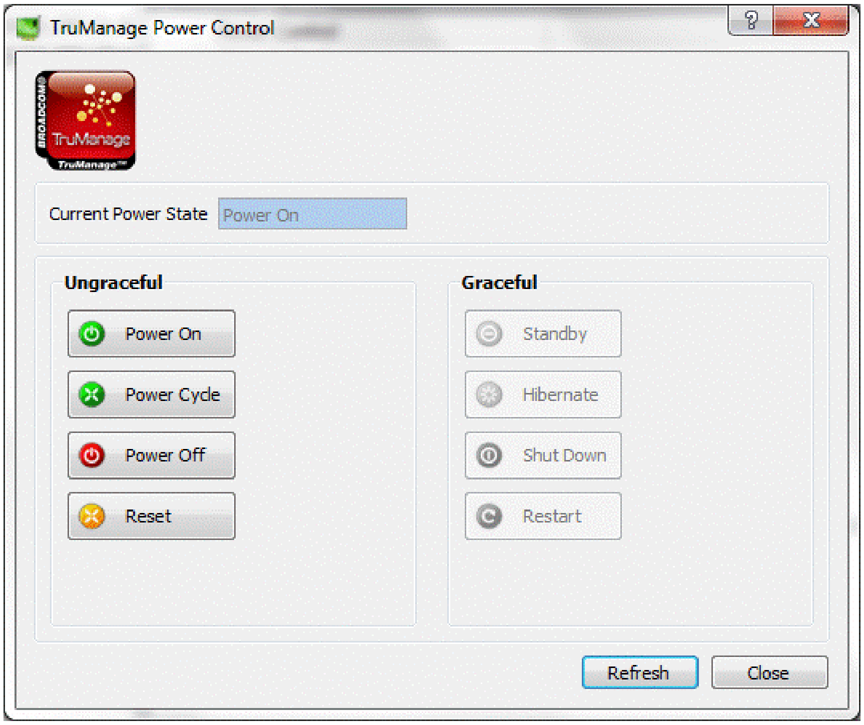
	Read	Write	Execute	Super	Audit
Base Desktop and Mobile	☑	☑	☑		
BIOS Management	☑	☑	☑		
Boot Control	☑	☑	☑		
Broadcom OOB Management Service	☑	☑	☑		
CPU	☑	☑	☑		
Fan	☑	☑	☑		
Indications	☑	☑	☑		
Network Quarantine	☑	☑	☑		
Opaque Management Data	☑	☑	☑	☑	
OS Status	☑	☑	☑		
Physical Asset	☑	☑	☑		
Power State Management	☑	☑	☑		

Managing the Power State

You can powered on, shut down, reset, or put in a sleep mode a managed system securely from the remote console. You can perform a system shut down or reset operation gracefully or ungracefully. The power control feature is essential during the remote diagnosis and repair of a system that fails to boot or run the OS.

To manage the power state

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Utilities** tab.
3. Filter the view by selecting **TruManage Tools**.
4. From **Power Control**, select **Launch Tool**. The **TruManage Power Control** window appears.
5. Select a power option, and then click **Refresh** to view the current power state.
6. Select **Close** to close the window.



Current Power State: Power On

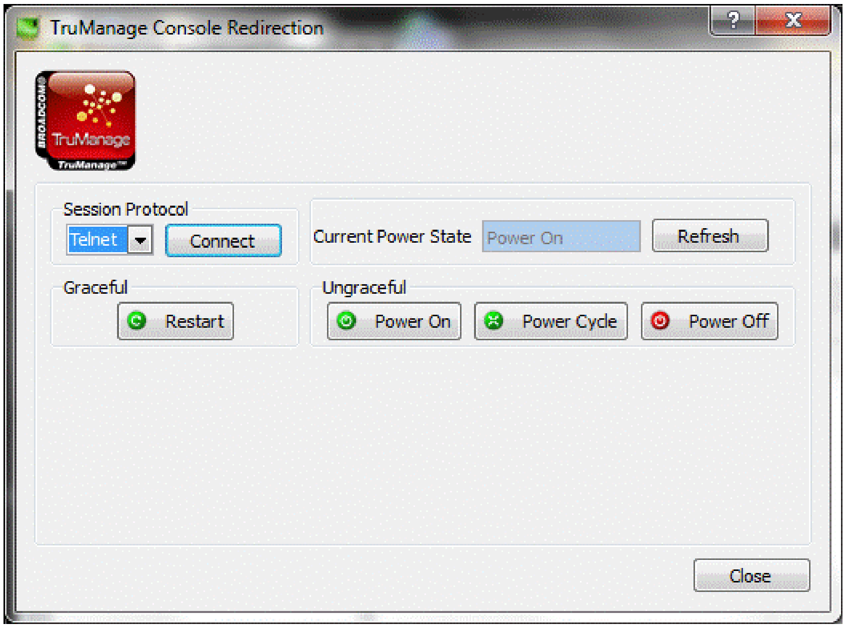
Monitoring and Managing a System

The ability to remotely monitor and administer a system without a local keyboard, mouse, and video monitor is important for handling the scenario when the system fails to boot or the OS fails to load. Text console redirection is a feature that allows for the text console I/O to be redirected to the remote management console. If you need to check or change the BIOS setting on a remote system, the text console redirection feature allows the BIOS menu screen (or any text console) to be redirected to the IT administrator's console. With the local keyboard being locked, the administrator can remotely reconfigure and reboot the system.

Note: Console Redirection may not be available for your managed system.

To monitor and manage a system

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Utilities** tab.
3. Filter the view by selecting **TruManage Tools**.
4. From **Console Redirection**, select **Launch Tool** and select **Connect**.
5. Select **Restart** or **Power Cycle** to restart the managed system. The **TruManage Console Redirection** window appears with the text stream from the managed system appearing in the TruManage Console Redirection window.
6. If at any time you need to change the power state, select a power option, and then click **Refresh** to view the current power state.
7. Select **Close** to close the window.



Session Protocol: Telnet
Current Power State: Power On
Graceful
Ungraceful

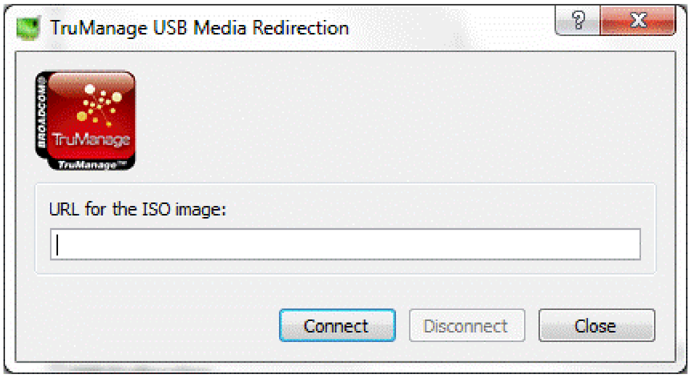
Booting From an ISO Image

USB Media Redirection is a tool that provides you with the ability to remotely boot a system when the local disk is corrupted or the system fails to boot. USB redirection allows you to boot from a remote ISO image using an HTTP-based protocol. The USB-redirected device appears as a virtual read-only mass-storage class USB device to the system firmware (BIOS) and OS. The redirection of the control/data to/from the virtual USB device is handled transparently using an HTTP-based redirection protocol. This feature enables remote booting, provisioning, re-imaging, and diagnostics while leveraging the existing USB plug-n-play capabilities. This eliminates desk-side visits and extends your accessibility to remote platforms.

Note: Console Redirection may not be available for your managed system.

To boot from an ISO image

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Utilities** tab.
3. Filter the view by selecting **TruManage Tools**.
4. From **USB Redirection**, select **Launch Tool**. The **TruManage USB Media Redirection** window appears. Ensure the management console can access the ISO image from http:\\<webserver>\<boot.iso>.
5. Type the location of the ISO image using the format http:\\<webserver>\<boot.iso> and click **Connect**.
6. From the **TruManage Power Control** window (see Managing the Power State), restart the managed system. The managed system will boot using the ISO image.
7. Select **Close** to close the window.

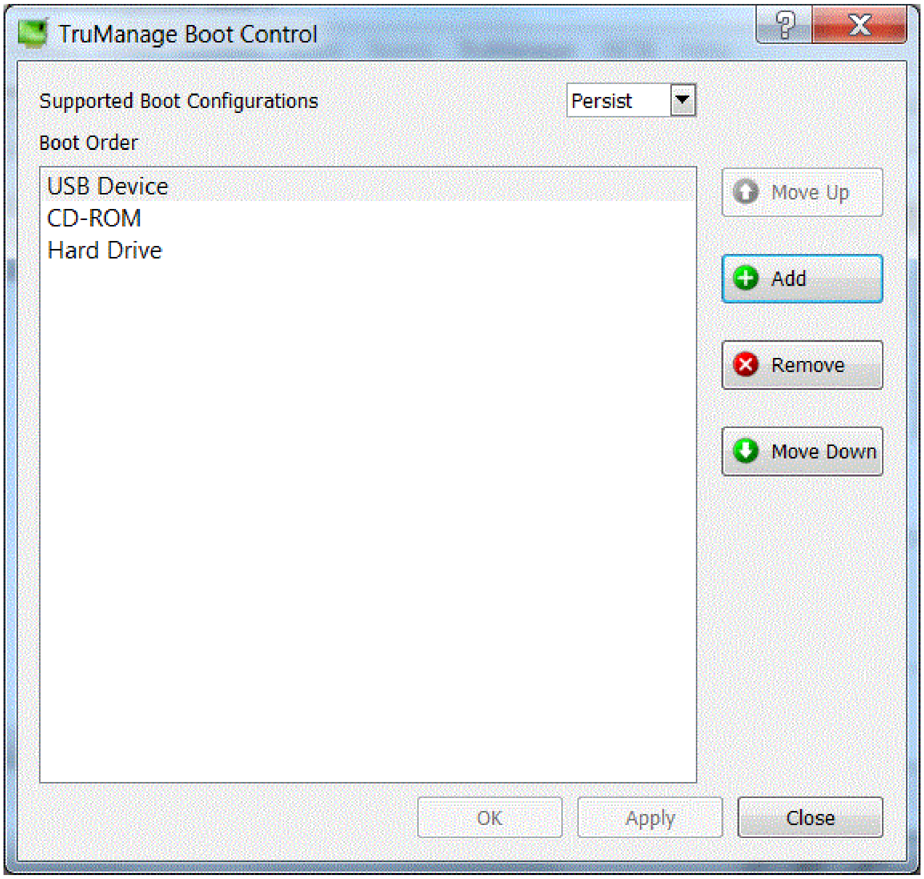


Managing the Boot

Both persistent and one-time boot configurations are supported. You can use different boot-source settings for different boot configurations. The remote boot control feature is useful for reimaging and/or repairing the system. For example, when an OS becomes unresponsive on a system, you can remotely reboot to a diagnostics environment to detect and analyze OS problems, successfully reimage the system with a new OS image, and reboot the system with the new OS.

To manage the boot

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Utilities** tab.
3. Filter the view by selecting **TruManage Tools**.
4. From **Boot Control**, select **Launch Tool**. The **TruManage Boot Control** window appears.
5. Add, remove, or change the boot order.
6. Select **Close** to close the window.


TruManage Boot Control

Supported Boot Configurations: Persist

Boot Order

USB Device
CD-ROM
Hard Drive

Managing Firmware Updates

The ability to update OOB management firmware using either in-band or an OOB environment allows the management console or an administrator to push fixes to the management firmware as well as update the firmware with new features.

To manage firmware updates

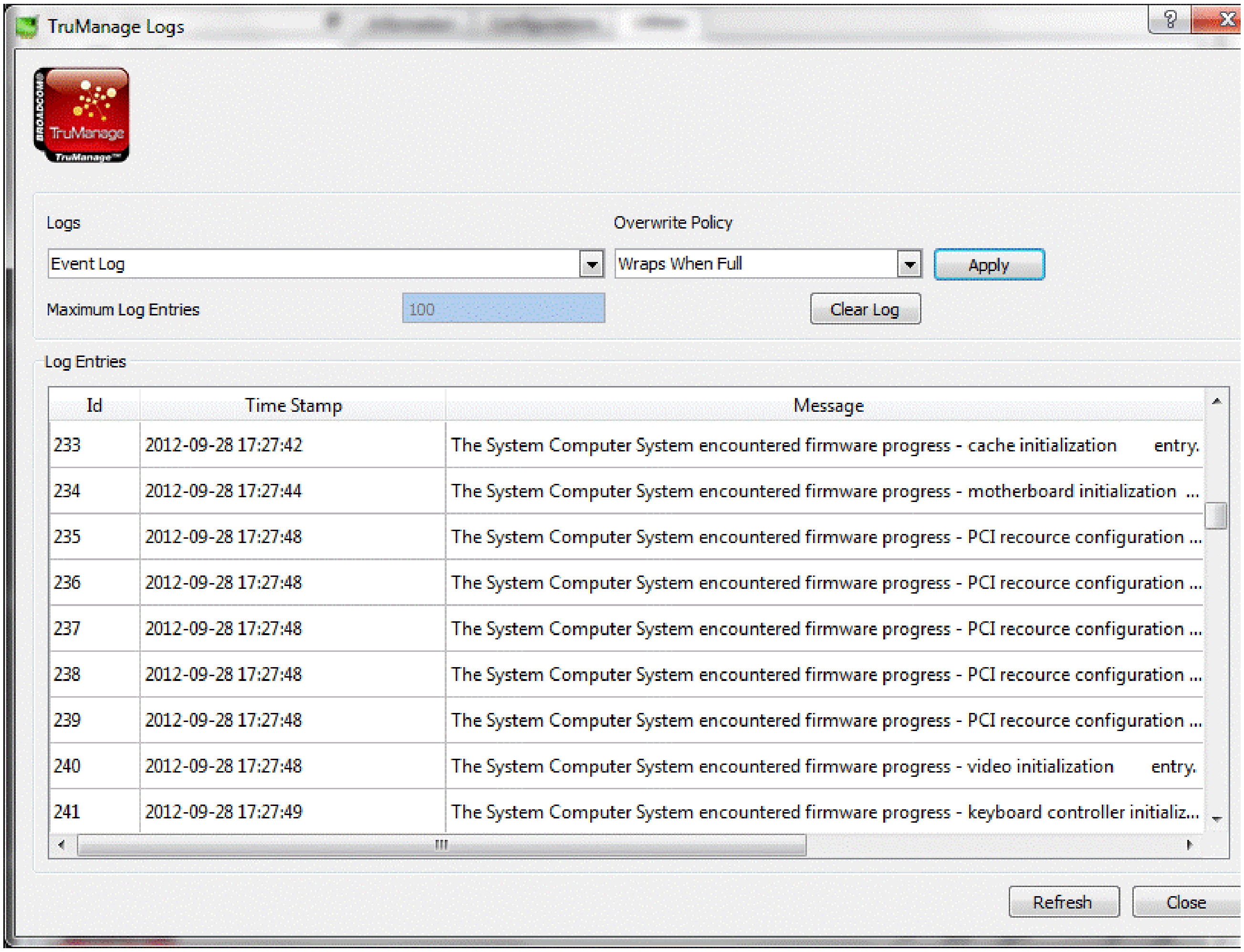
1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Utilities** tab.
3. Filter the view by selecting **TruManage Tools**.
4. From **Firmware Updates**, select **Launch Tool**. The **TruManage Firmware Updates** window appears.
5. Select **Close** to close the window.

Viewing Event Log

This feature provides a log of alert-indication related information. This log can be read and cleared. It allows you to have visibility into the events that happened inside the system. The event logging feature enhances the ability to monitor and diagnose a system.

To view event logs

1. From the management console, run BACS in administrator mode and ensure the view filter is set to **TRUMANAGE VIEW**.
2. Select the **Utilities** tab.
3. Filter the view by selecting **TruManage Tools**.
4. From **Logs**, select **Launch Tool**. The **TruManage Logs** window appears.
5. Select the log to view.
6. Change log preferences or clear the log.
7. Select **Close** to close the window.



Logs: Event Log

Overwrite Policy: Wraps When Full

Maximum Log Entries: 100

Log Entries

Id	Time Stamp	Message
233	2012-09-28 17:27:42	The System Computer System encountered firmware progress - cache initialization entry.
234	2012-09-28 17:27:44	The System Computer System encountered firmware progress - motherboard initialization ...
235	2012-09-28 17:27:48	The System Computer System encountered firmware progress - PCI recource configuration ...
236	2012-09-28 17:27:48	The System Computer System encountered firmware progress - PCI recource configuration ...
237	2012-09-28 17:27:48	The System Computer System encountered firmware progress - PCI recource configuration ...
238	2012-09-28 17:27:48	The System Computer System encountered firmware progress - PCI recource configuration ...
239	2012-09-28 17:27:48	The System Computer System encountered firmware progress - PCI recource configuration ...
240	2012-09-28 17:27:48	The System Computer System encountered firmware progress - video initialization entry.
241	2012-09-28 17:27:49	The System Computer System encountered firmware progress - keyboard controller initializ...

VIEWING STATISTICS

The information provided on the Statistics tab allows you to view traffic statistics for both Broadcom network adapters and network adapters made by others. Statistical information and coverage are more comprehensive for Broadcom adapters.

To view Statistics information for any installed network adapter, click the name of the adapter listed in the Explorer View pane, then click the Statistics tab.

Click **Refresh** to get the most recent values for each statistic. Click **Reset** to change all values to zero.

NOTES:

- Team statistics are not compiled for a Broadcom network adapter if it is disabled.
- Some statistics may not be available for all Broadcom network adapters.

GENERAL STATISTICS

General Statistics show the transmitted and received statistics to and from the adapter.

Frames Tx OK. A count of the frames that were successfully transmitted. This counter is incremented when the transmit status is reported as Transmit OK.

Frames Rx OK. A count of the frames that were successfully received. This does not include frames received with frame-too-long, frame check sequence (FCS), length, or alignment errors, nor frames lost due to internal MAC sublayer errors. This counter is incremented when the receive status is reported as Receive OK.

Directed Frames Tx. A count of directed data frames that were successfully transmitted.

Multicast Frames Tx. A count of frames that were successfully transmitted (as indicated by the status value Transmit OK) to a group destination address other than a broadcast address.

Broadcast Frames Tx. A count of frames that were successfully transmitted (as indicated by the transmit status Transmit OK) to the broadcast address. Frames transmitted to multicast addresses are not broadcast frames and are excluded.

Directed Frames Rx. A count of directed data frames that were successfully received.

Multicast Frames Rx. A count of frames that were successfully received and are directed to an active nonbroadcast group address. This does not include frames received with frame-too-long, FCS, length, or alignment errors, nor frames lost because of internal MAC sublayer errors. This counter is incremented as indicated by the Receive OK status.

Broadcast Frames Rx. A count of frames that were successfully received and are directed to a broadcast group address. This count does not include frames received with frame-too-long, FCS, length, or alignment errors, nor frames lost because of internal MAC sublayer errors. This counter is incremented as indicated by the Receive OK status.

Frames Rx with CRC Error. The number of frames received with CRC errors.

The total number of offloaded TCP connections.

Configuring Teaming

NOTE: BACS does not support teaming on Linux systems.

The teaming function allows you to group any available network adapters together to function as a team. Teaming is a method of creating a virtual NIC (a group of multiple adapters that functions as a single adapter). The benefit of this approach is that it enables load balancing and failover. Teaming is done through the Broadcom Advanced Server Program (BASP) software. For a comprehensive description of the technology and implementation considerations of the teaming software, refer to the "Broadcom Gigabit Ethernet Teaming Services" section of your Broadcom network adapter user guide.

Teaming can be accomplished by either of the following methods:

- Using the Broadcom Teaming Wizard
- Using Expert Mode

NOTES:

- For further information regarding teaming protocols, see “Teaming” in your Broadcom network adapter user guide.
- If you do not enable LiveLink™ when configuring teams, disabling Spanning Tree Protocol (STP) at the switch is recommended. This minimizes the downtime due to spanning tree loop determination when failing over. LiveLink mitigates such issues.
- BASP is available only if a system has one or more Broadcom network adapters installed.
- To physically remove a teamed NIC from a system, you must first delete the NIC from the team. Not doing this before shutting down the system could result in breaking the team on a subsequent reboot, which may result in unexpected team behavior.
- The Large Send Offload (LSO) and Checksum Offload properties are enabled for a team only when all of the members support and are configured for the feature.
- You must have administrator privileges to create or modify a team.
- The load balance algorithm in a team environment in which members are connected at different speeds favors members connected with a Gigabit Ethernet link over members connected at lower speed links (100 Mbps or 10 Mbps) until a threshold is met. This is normal behavior.
- Wake on LAN (WOL) is a feature that allows a system to be awakened from a sleep state by the arrival of a specific packet over the Ethernet interface. Because a virtual adapter is implemented as a software only device, it lacks the hardware features to implement WOL and cannot be enabled to wake the system from a sleeping state via the virtual adapter. The physical adapters, however, support this property, even when the adapter is part of a team.

TEAM TYPES

You can create four types of load balance teams:

- Smart Load Balance and Failover
- Link Aggregation (802.3ad)
- Generic Trunking (FEC/GEC)/802.3ad-Draft Static
- SLB (Auto-Fallback Disable) – The Auto-Fallback Disable feature is configured for Smart Load Balance and Failover type teams in the Teaming Wizard.

Smart Load Balance and Failover

In this type of team, a standby member handles the traffic if all of the load balance members fail (a failover event). All load balance members have to fail before the standby member takes over. When one or more of the load balance members is restored (fallback), the restored team member(s) resumes the handling of the traffic. The LiveLink feature is supported for this type of team.

Link Aggregation (802.3ad)

In this type of team, you can dynamically configure the network adapters that have been selected to participate in a given team. If the link partner is not correctly configured for IEEE 802.3ad link configuration, errors are detected and noted. All adapters in the team are configured to receive packets for the same MAC address. The outbound load balancing scheme is determined by the BASP driver. The link partner of the team determines the load balancing scheme for inbound packets. In this mode, at least one of the link partners must be in active mode.

Generic Trunking (FEC/GEC)/802.3ad-Draft Static

This type of team is very similar to the link aggregation type, in that all adapters in the team must be configured to receive packets for the same MAC address. This mode does not provide link aggregation control protocol (LACP) or marker protocol support. This mode supports a variety of environments where the link partners are statically configured to support a proprietary trunking mechanism. Trunking supports load balancing and failover for both outbound and inbound traffic.

SLB (Auto-Fallback Disable)

This team is identical to Smart Load Balance and Failover, with the following exception: when the standby member is active, if a primary member comes back online, the team continues using the standby member rather than switching back to the primary member. This type of team is supported only for situations in which the network cable is disconnected and reconnected to the network adapter. It is not supported for situations in which the adapter is removed/installed through Device Manager or Hot-Plug PCI. If any primary adapter assigned to a team is disabled, the team functions as a Smart Load Balancing and Failover type of team in which auto-fallback occurs. The LiveLink feature is supported for this type of team.

Standby Team Member and Auto-Fallback Disable Mode

You can designate one team member in an SLB type of team to be the standby member. The standby member does not actively send and receive normal network traffic while other adapters on the team are active. If all of the active adapters on the team fail or are disconnected, the standby member takes over the handling of the network activities.

In Auto-Fallback Disable mode, if a load balance member returns on line, the team continues using the standby member rather than switching back to using the load balance member. Consequently, the adapter that was initially designated a load balance member remains in an inactive state and becomes the new standby member.

LiveLink

LiveLink is a feature of BASP that is available for the Smart Load Balancing (SLB) and SLB (Auto-Fallback Disable) type of teaming. The purpose of LiveLink is to detect link loss beyond the switch and to route traffic only through team members that have a live link.

Using the Broadcom Teaming Wizard

You can use the Broadcom Teaming Wizard to create a team, configure an existing team if a team has already been created, or create a VLAN.

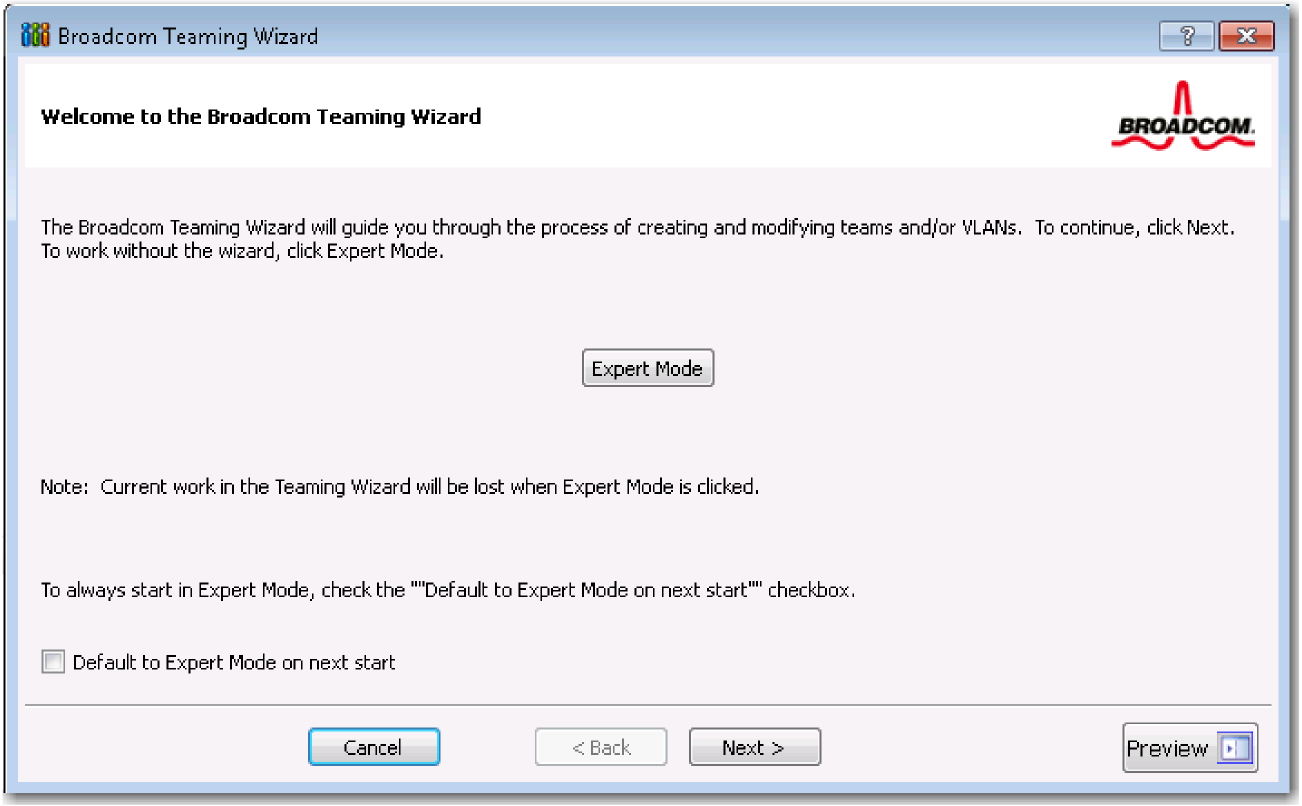
1. Create or edit a team:

   To create a new team, select **Create a Team** from the **Team** menu, or right-click one of the devices in the "Unassigned Adapters" section and select **Create a Team**. This option is not available if there are no devices listed in the "Unassigned Adapters" sections, which means all adapters are already assigned to teams.

   To configure an existing team, right-click one of the teams in the list and select **Edit Team**. This option is only available if a team has already been created and is listed in the Team Management pane.

   Note: If you prefer to work without the wizard for now, click **Expert Mode**. If you want to always use Expert Mode to create a team, select **Default to Expert Mode on next start**. See Using Expert Mode.

2. To continue using the wizard, click **Next**.



Welcome to the Broadcom Teaming Wizard

The Broadcom Teaming Wizard will guide you through the process of creating and modifying teams and/or VLANs. To continue, click Next. To work without the wizard, click Expert Mode.

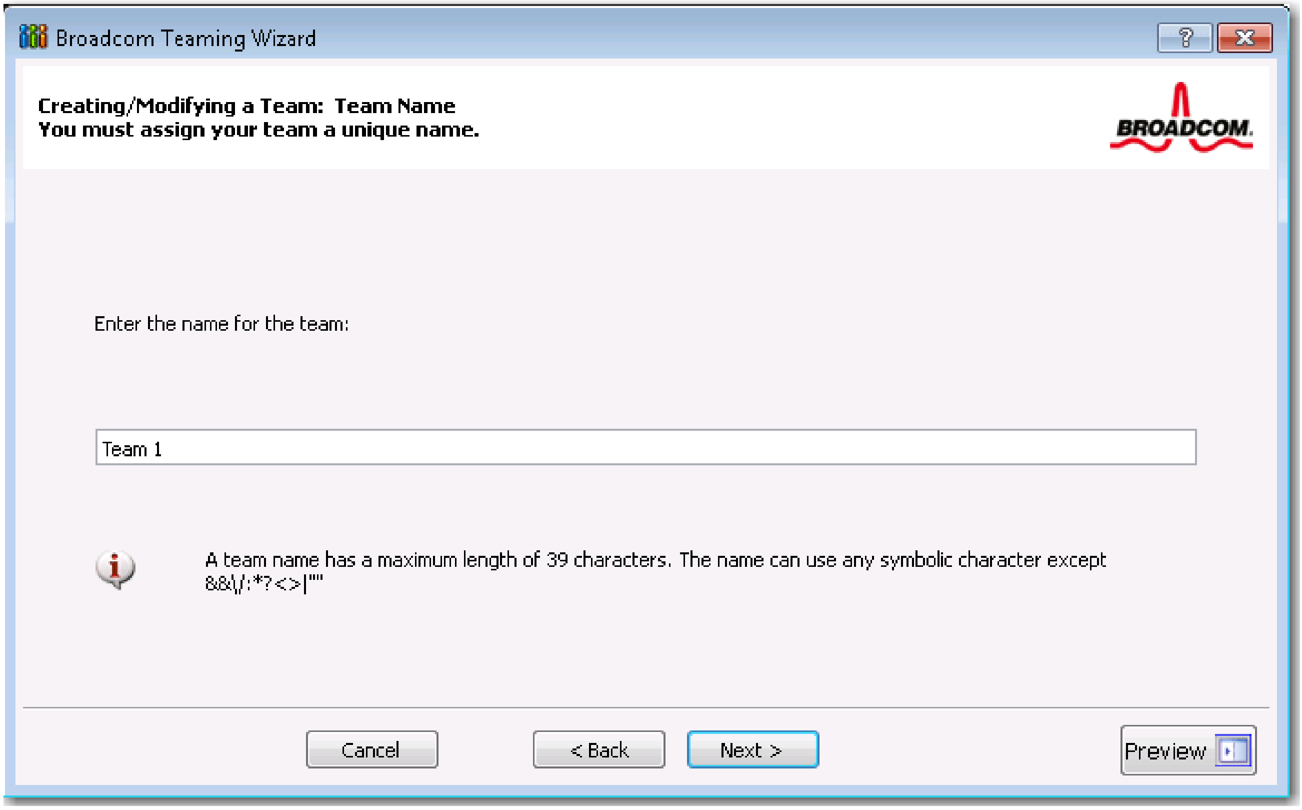
Note: Current work in the Teaming Wizard will be lost when Expert Mode is clicked.

To always start in Expert Mode, check the ""Default to Expert Mode on next start"" checkbox.

□ Default to Expert Mode on next start

3. Type the team name and then click **Next**. If you want to review or change any of your settings, click **Back**. Click **Cancel** to discard your settings and exit the wizard.

Note: The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |



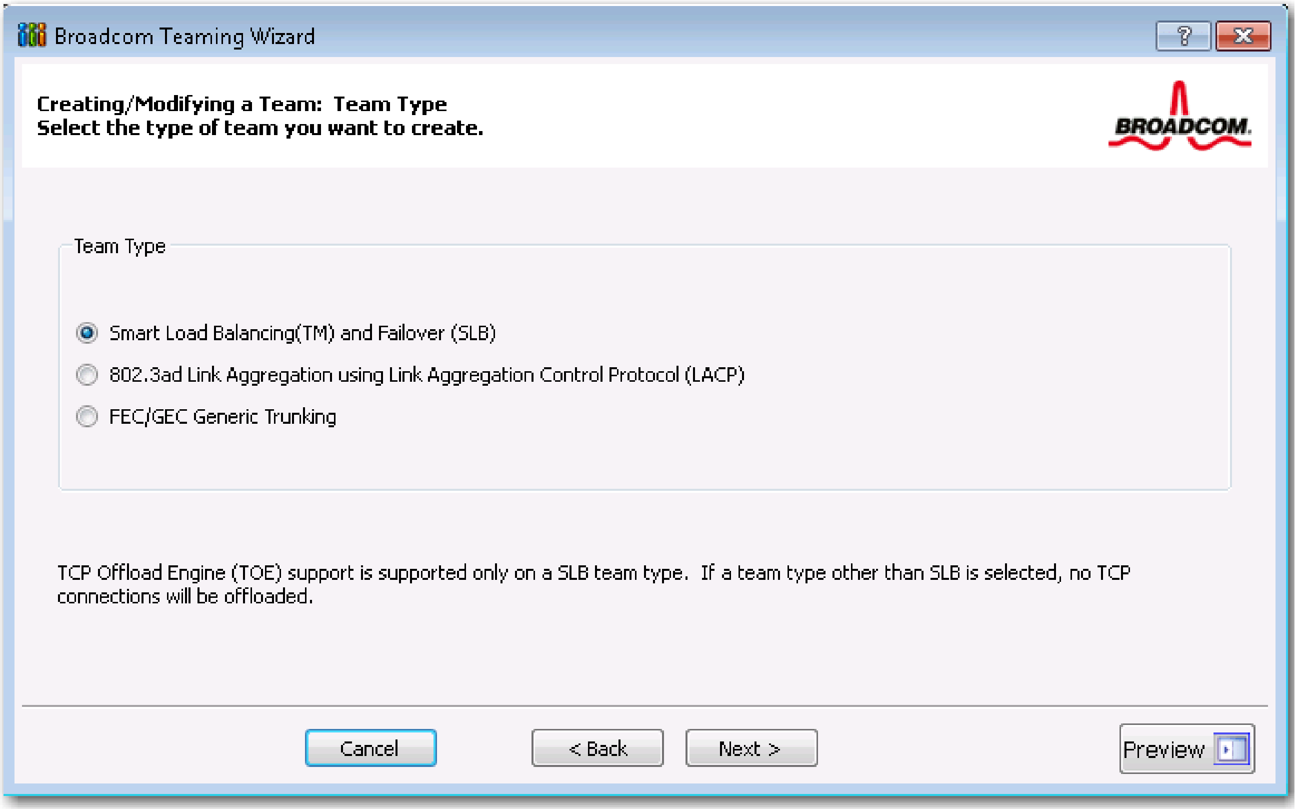
Creating/Modifying a Team: Team Name
You must assign your team a unique name.

Enter the name for the team:

Team 1

A team name has a maximum length of 39 characters. The name can use any symbolic character except &&\/:*?<>|""

4. Select the type of team you want to create. If the team type is an SLB type team, click **Next**. If the team type is not an SLB type team, then a dialog box appears. Verify that the network switch connected to the team members is configured correctly for the team type, click **OK**, and continue.



Broadcom Teaming Wizard

Creating/Modifying a Team: Team Type
Select the type of team you want to create.

Team Type

● Smart Load Balancing(TM) and Failover (SLB)

○ 802.3ad Link Aggregation using Link Aggregation Control Protocol (LACP)

○ FEC/GEC Generic Trunking

TCP Offload Engine (TOE) support is supported only on a SLB team type. If a team type other than SLB is selected, no TCP connections will be offloaded.

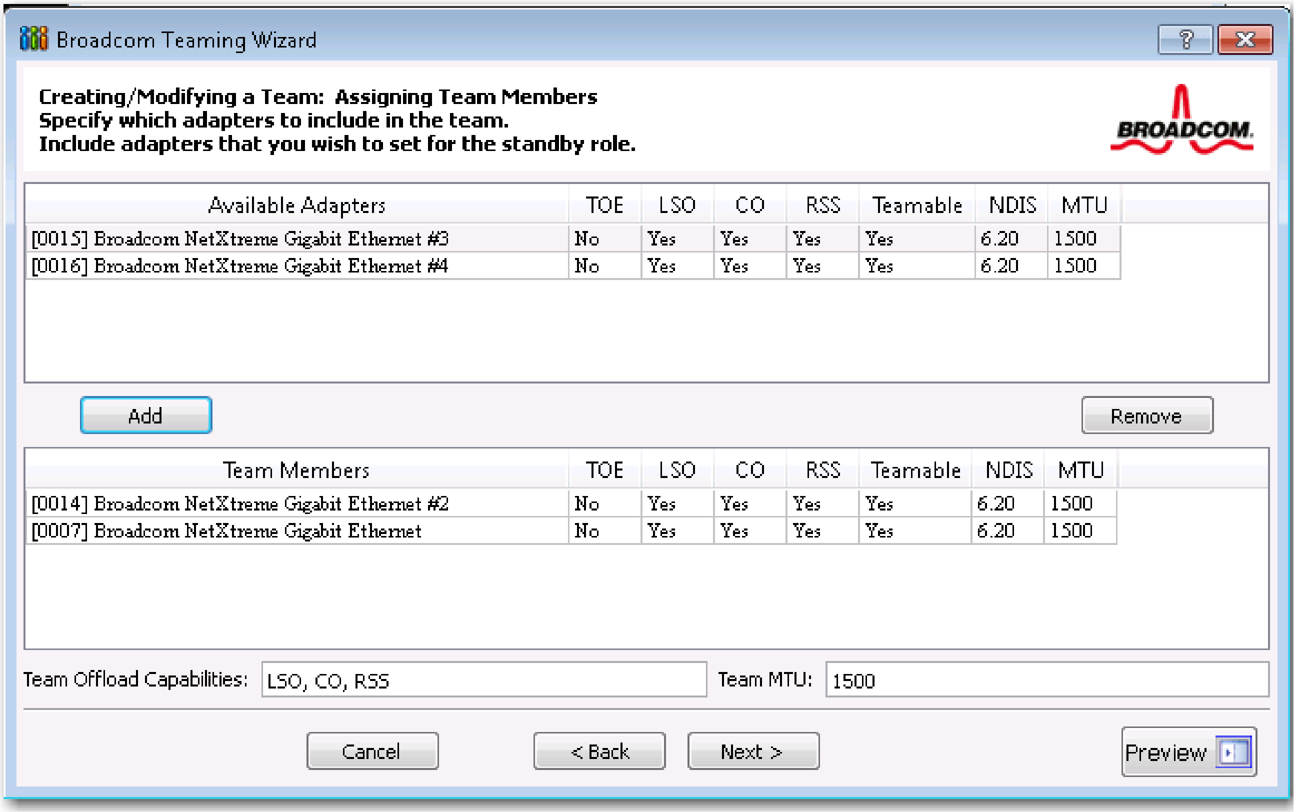
5. From the **Available Adapters** list, click the adapter you want to add to the team and then click **Add**. Remove team members from the **Team Members** list by clicking the adapter and then clicking **Remove**. Click **Next**.

Note: There must be at least one Broadcom network adapter assigned to the team.

The TCP Offload Engine (TOE), Large Send Offload (LSO) and Checksum Offload (CO) columns indicate if the TOE, LSO, and/or the CO properties are supported for the adapter. The TOE, LSO, and CO properties are enabled for a team only when all of the members support and are configured for the feature. If this is the case, then the team offload capabilities appear on the bottom of the screen.

NOTES:

- Adding a network adapter to a team where its driver is disabled may negatively affect the offloading capabilities of the team. This may have an impact on the team's performance. Therefore, it is recommended that only driver-enabled network adapters be added as members to a team.



Creating/Modifying a Team: Assigning Team Members
Specify which adapters to include in the team.
Include adapters that you wish to set for the standby role.

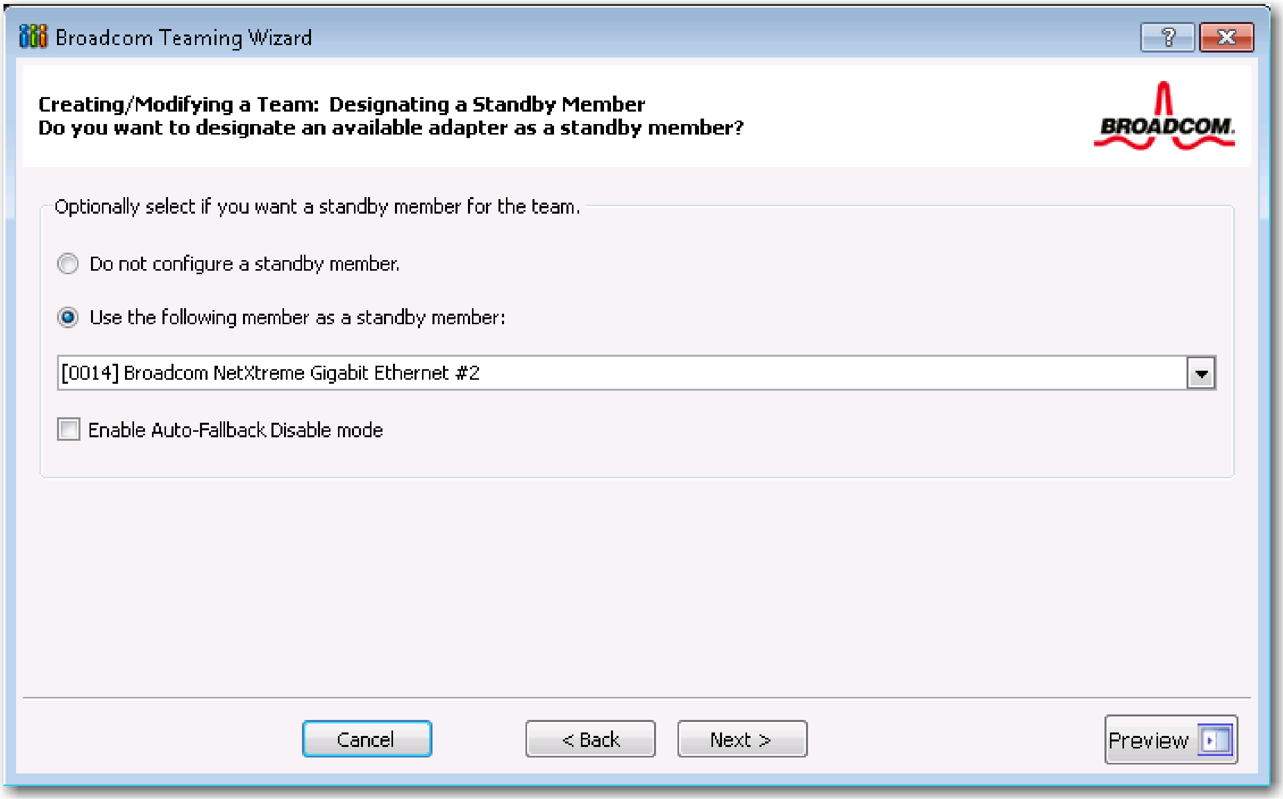
Available Adapters	TOE	LSO	CO	RSS	Teamable	NDIS	MTU
[0015] Broadcom NetXtreme Gigabit Ethernet #3	No	Yes	Yes	Yes	Yes	6.20	1500
[0016] Broadcom NetXtreme Gigabit Ethernet #4	No	Yes	Yes	Yes	Yes	6.20	1500

Team Members	TOE	LSO	CO	RSS	Teamable	NDIS	MTU
[0014] Broadcom NetXtreme Gigabit Ethernet #2	No	Yes	Yes	Yes	Yes	6.20	1500
[0007] Broadcom NetXtreme Gigabit Ethernet	No	Yes	Yes	Yes	Yes	6.20	1500

Team Offload Capabilities: LSO, CO, RSS

Team MTU: 1500

6. If you want to designate one of the adapters as a standby member (optional), select **Use the following member as a standby member**, then choose the standby member from the list of adapters.
7. The Auto-Fallback Disable mode feature allows the team to continue using the standby member rather than switching back to the primary member if the primary member comes back online. To enable this feature, select **Enable Auto-Fallback Disable mode**. Click **Next**.



Broadcom Teaming Wizard

Creating/Modifying a Team: Designating a Standby Member
Do you want to designate an available adapter as a standby member?

Optionally select if you want a standby member for the team.

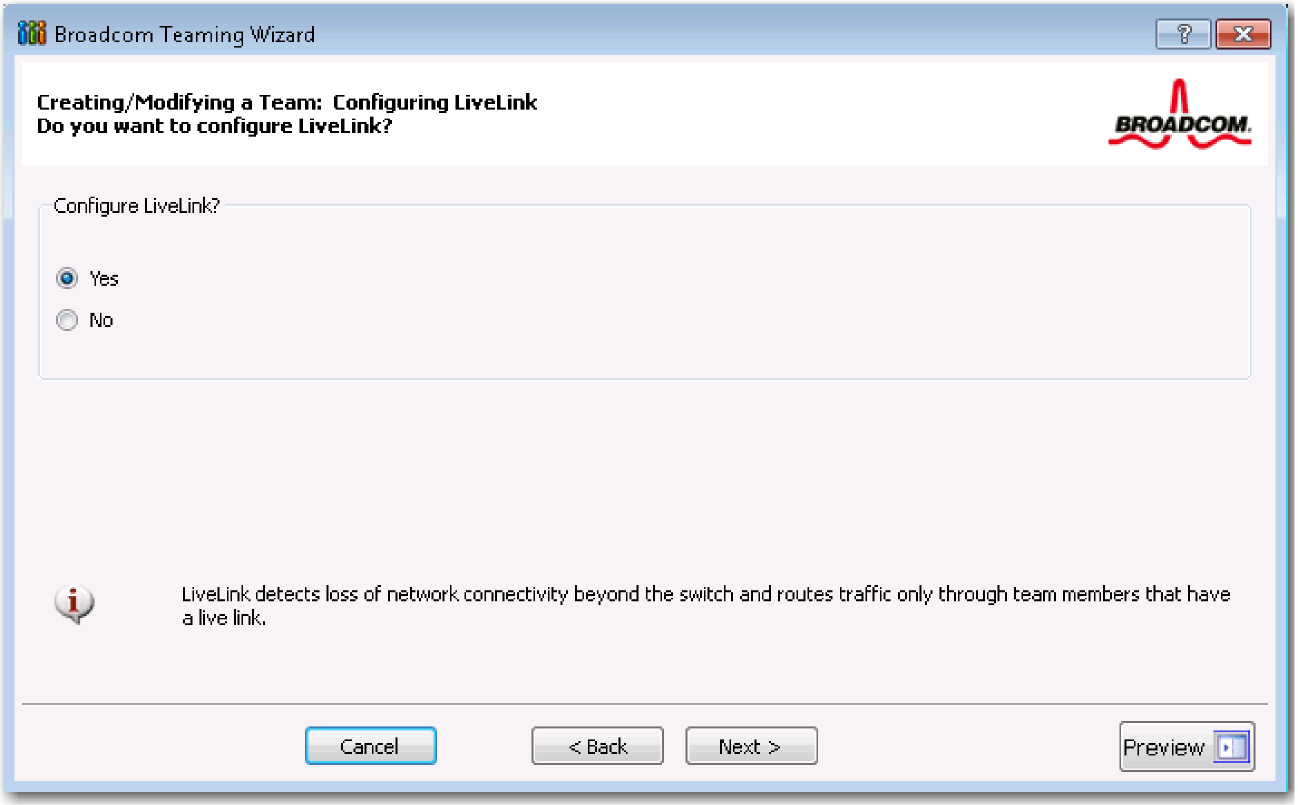
○ Do not configure a standby member.

● Use the following member as a standby member:

[0014] Broadcom NetXtreme Gigabit Ethernet #2

□ Enable Auto-Fallback Disable mode

8. If you want to configure LiveLink, select **Yes**, otherwise select **No**, then click **Next**.



Creating/Modifying a Team: Configuring LiveLink
Do you want to configure LiveLink?

Configure LiveLink?

● Yes
○ No

LiveLink detects loss of network connectivity beyond the switch and routes traffic only through team members that have a live link.

9. Select the probe interval (the number of seconds between each retransmission of a link packet to the probe target) and the maximum number of probe retries (the number of consecutively missed responses from a probe target before a failover is triggered).

10. Set the Probe VLAN ID to allow for connectivity with probe targets residing on a tagged VLAN. The number set must match the VLAN ID of the probe targets as well as the port(s) on the switch to which the team is connected.

Note: Each LiveLink enabled team can only communicate with Probe Targets on a single VLAN. Also, VLAN ID 0 is equivalent to an untagged network. If the Probe VLAN ID is set to a value other than 0, then a VLAN must be created with an identical VLAN tag value (see Step 16. on page 206).

11. Click the probe target at the top of the list, click **Edit Target IP Address**, type the target IP address in the **IP Address** box for one or all probe targets, and then click **OK**. Click **Next**.

Note: Only the first probe target is required. You can specify up to three additional probe targets to serve as backups by assigning IP addresses to the other probe targets.

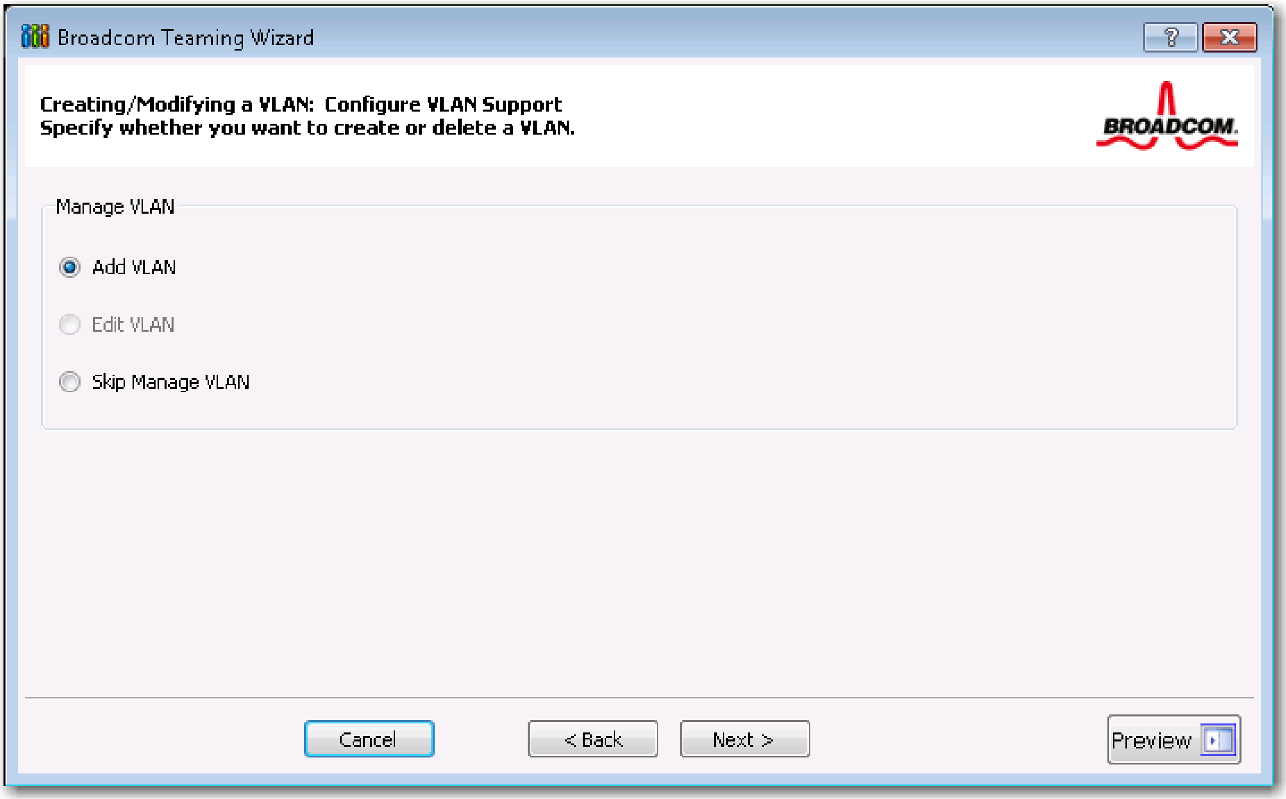
12. Select a listed team member, click **Edit Member IP Address**, and then type the member IP address in the IP Address box. Repeat for all listed team members and then click **OK**. Click **Next**.

Note: All of the member IP addresses must be in the same subnet as the subnet of the probe targets.

13. If you want to create a VLAN on the team, select **Add VLAN**, or if you want to change the settings of an existing VLAN, select **Edit VLAN**, then click **Next**. If you do not want to create or edit a VLAN, select **Skip Manage VLAN**, then click **Next**, and continue with the wizard from the Finish screen (see Step 18. on page 209 of this procedure).

VLANs enable you to add multiple virtual adapters that are on different subnets. The benefit of this is that your system can have one network adapter that can belong to multiple subnets.

Note: VLANs can only be created when all team members are Broadcom adapters.



Broadcom Teaming Wizard

Creating/Modifying a VLAN: Configure VLAN Support
Specify whether you want to create or delete a VLAN.

Manage VLAN

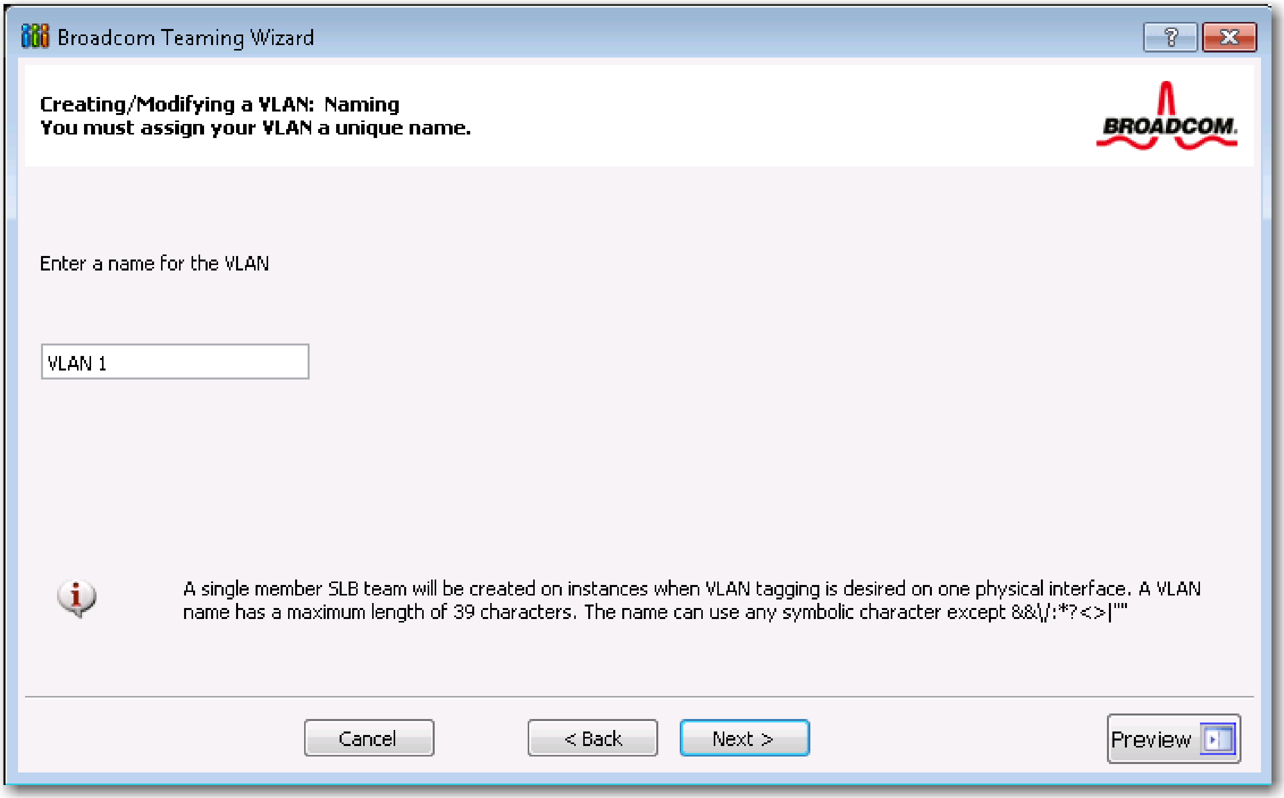
● Add VLAN

○ Edit VLAN

○ Skip Manage VLAN

14. Type the VLAN name and then click **Next**.

Note: The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |



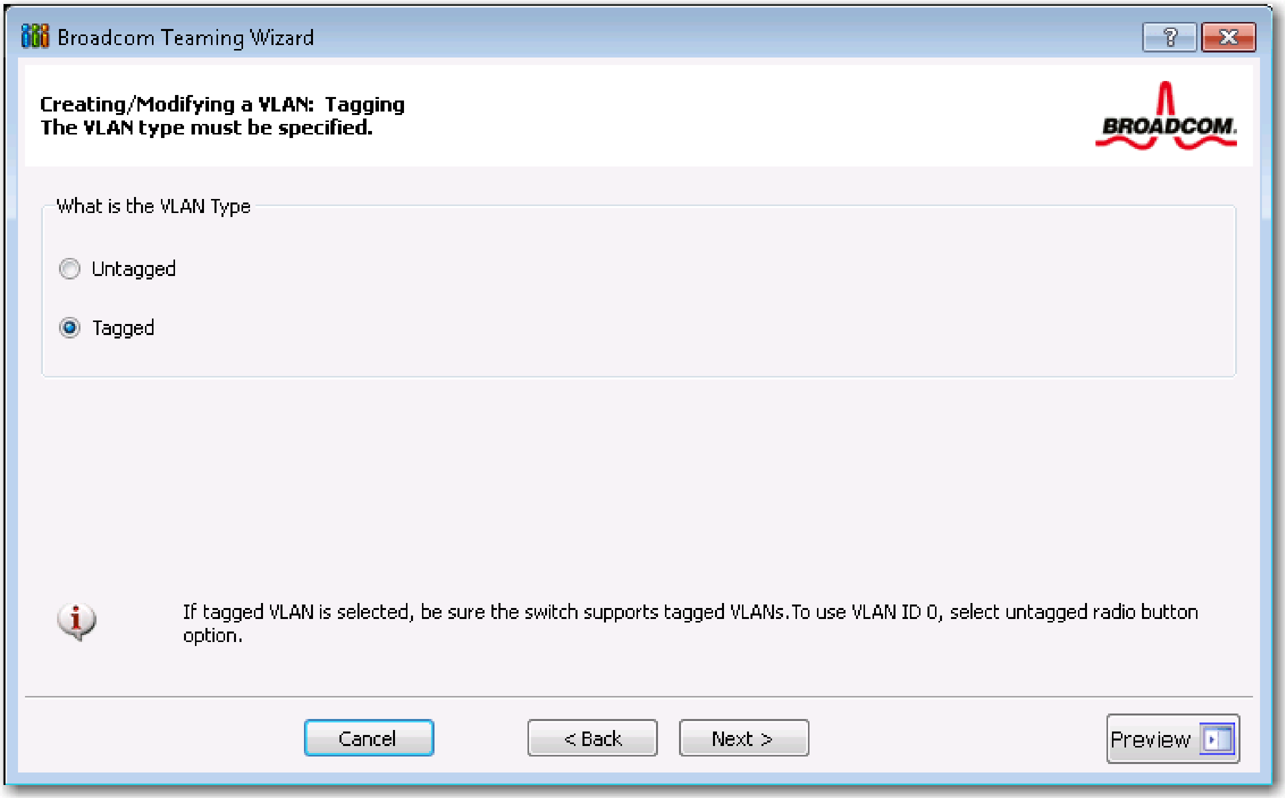
Creating/Modifying a VLAN: Naming
You must assign your VLAN a unique name.

Enter a name for the VLAN

VLAN 1

A single member SLB team will be created on instances when VLAN tagging is desired on one physical interface. A VLAN name has a maximum length of 39 characters. The name can use any symbolic character except &&\/:*?<>|""

15. To tag the VLAN, select **Tagged** and then click **Next**. Otherwise, click **Untagged**, click **Next**, and continue with the wizard to add additional VLANs (see Step 17. on page 208 of this procedure).



Creating/Modifying a VLAN: Tagging
The VLAN type must be specified.

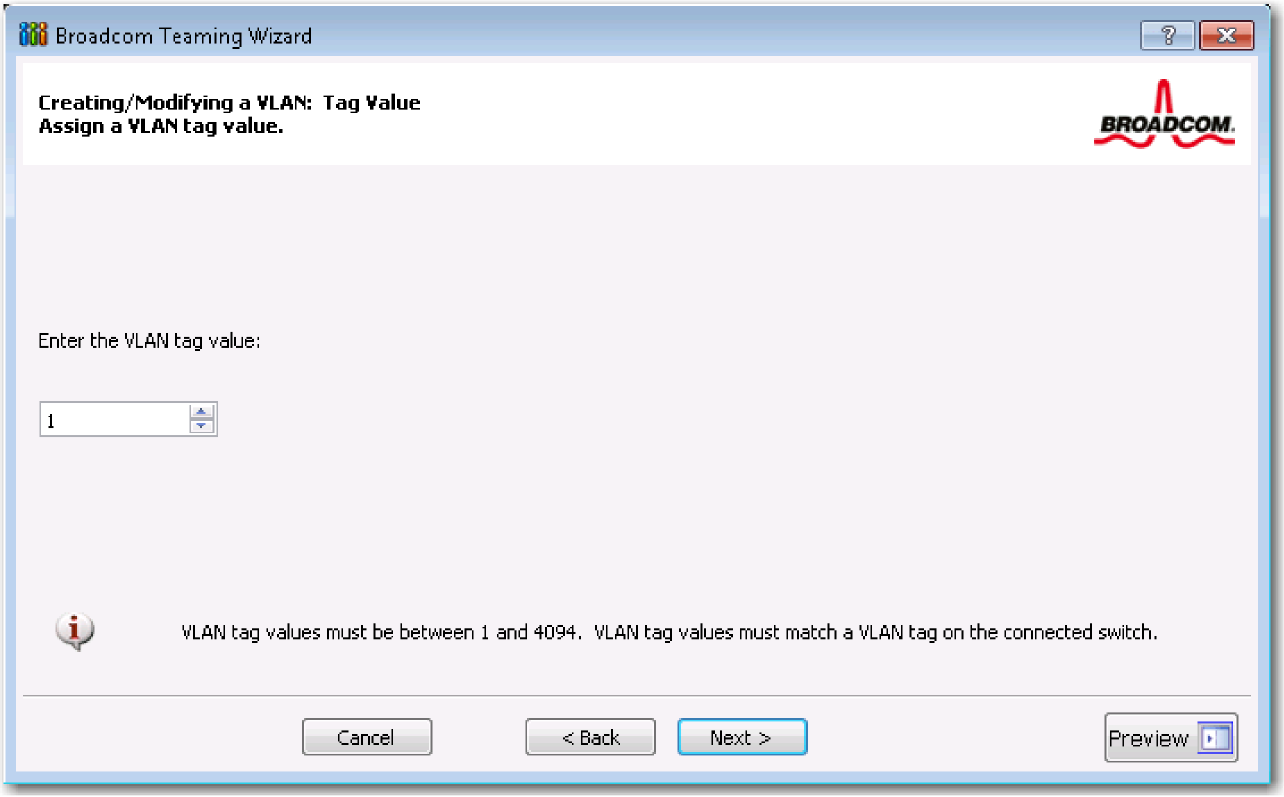
What is the VLAN Type

○ Untagged

● Tagged

If tagged VLAN is selected, be sure the switch supports tagged VLANs.To use VLAN ID 0, select untagged radio button option.

16. Type the VLAN tag value and then click **Next**. The value must be between 1 and 4094.



Creating/Modifying a VLAN: Tag Value
Assign a VLAN tag value.

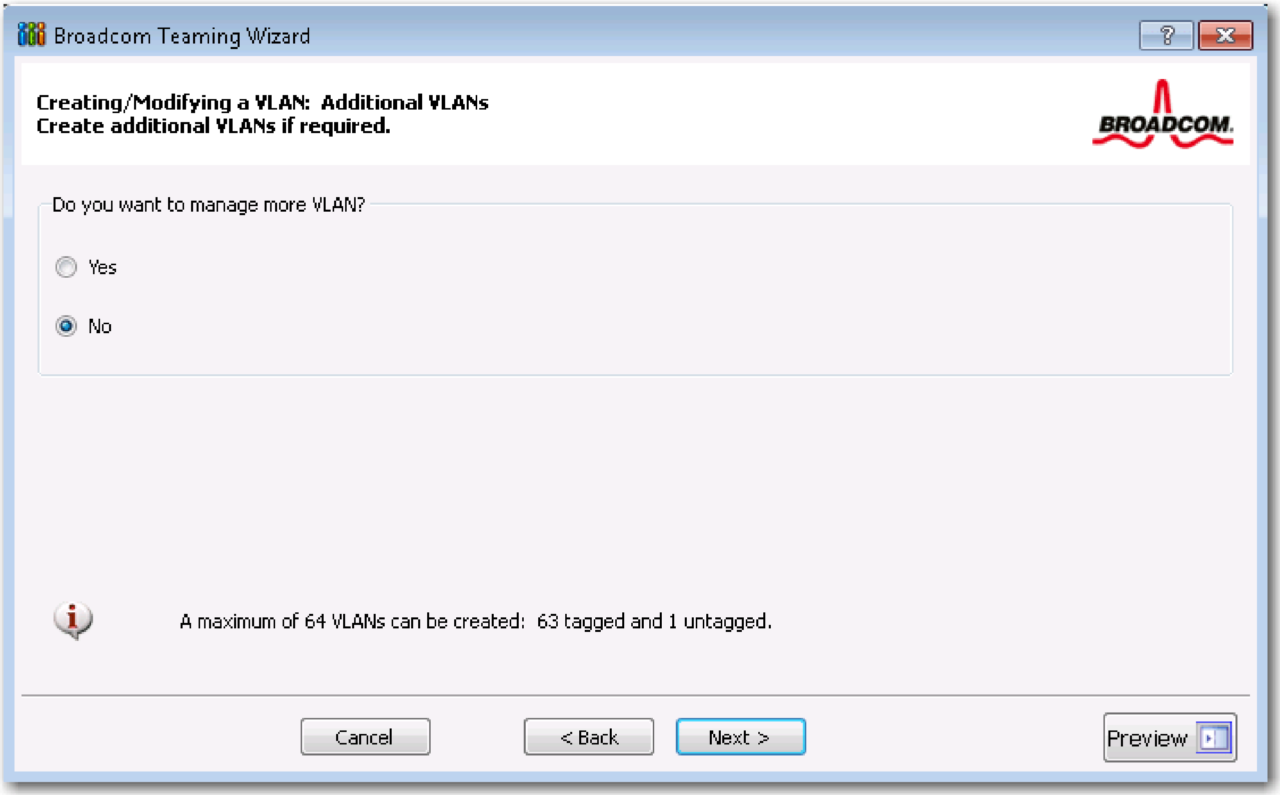
Enter the VLAN tag value:

1

VLAN tag values must be between 1 and 4094. VLAN tag values must match a VLAN tag on the connected switch.

17. Select **Yes** to add or manage another VLAN and then click **Next**. Repeat until you do not want to add or manage any additional VLANs.

Note: You can define up to 64 VLANs per team (63 VLANs that are tagged and 1 VLAN that is not tagged). Adding several VLANS may slow down the reaction time of the Windows interface due to memory and processor time usage for each VLAN. The degree to which Windows performance may suffer depends on system configuration.



Creating/Modifying a VLAN: Additional VLANs
Create additional VLANs if required.

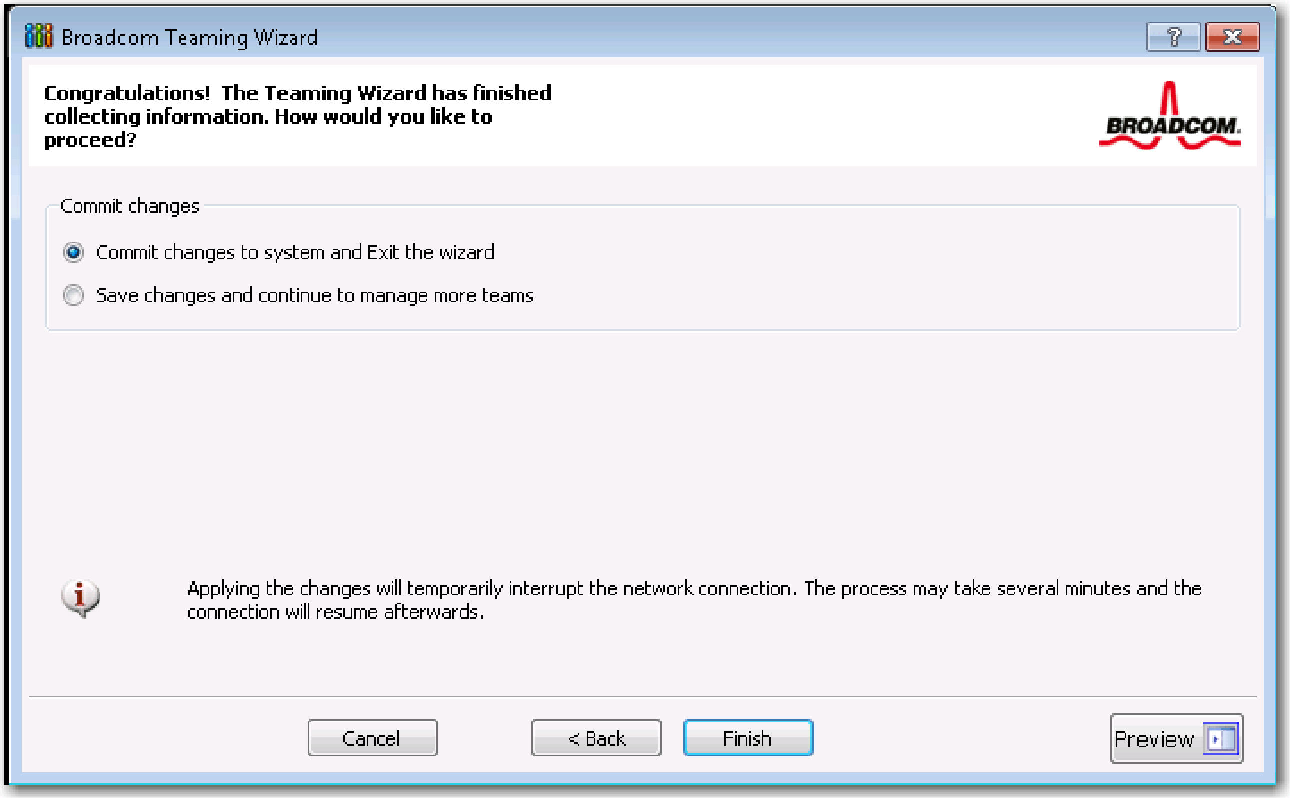
Do you want to manage more VLAN?

○ Yes

● No

A maximum of 64 VLANs can be created: 63 tagged and 1 untagged.

18. To apply and commit the changes to the team, select **Commit changes to system and Exit the wizard**. To apply your changes but continue using the wizard, select **Save changes and continue to manage more teams**. Click Finish.



Broadcom Teaming Wizard

Congratulations! The Teaming Wizard has finished collecting information. How would you like to proceed?

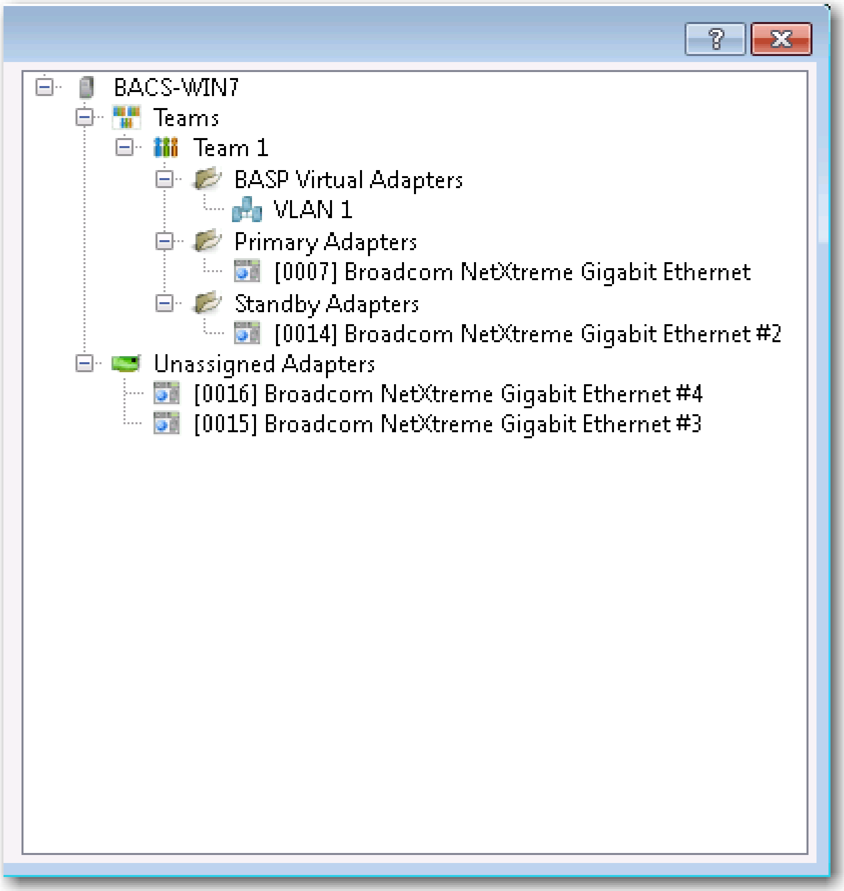
Commit changes

● Commit changes to system and Exit the wizard

○ Save changes and continue to manage more teams

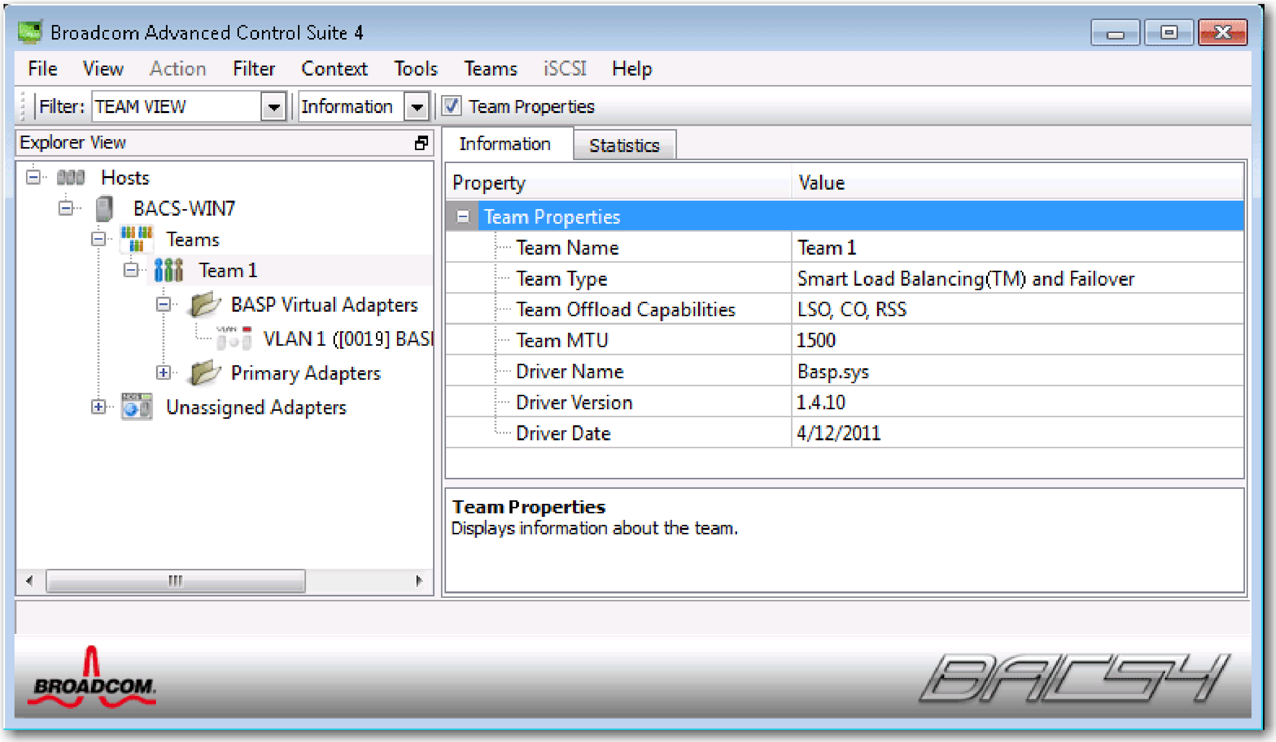
Applying the changes will temporarily interrupt the network connection. The process may take several minutes and the connection will resume afterwards.

Note: At any point in the Broadcom Teaming Wizard procedure, click **Preview** to get a visual representation of what the team will look like before committing any changes.



BACS-WIN7
- Teams
  - Team 1
    - BASP Virtual Adapters
      - VLAN 1
    - Primary Adapters
      - [0007] Broadcom NetXtreme Gigabit Ethernet
    - Standby Adapters
      - [0014] Broadcom NetXtreme Gigabit Ethernet #2
- Unassigned Adapters
  - [0016] Broadcom NetXtreme Gigabit Ethernet #4
  - [0015] Broadcom NetXtreme Gigabit Ethernet #3

19. Click the team name in the Team Management pane to view the team's properties in the **Information** tab, transfer and receive data in the **Statistics** tab.



Filter: TEAM VIEW

☑ Team Properties

Property	Value
Team Properties	
Team Name	Team 1
Team Type	Smart Load Balancing(TM) and Failover
Team Offload Capabilities	LSO, CO, RSS
Team MTU	1500
Driver Name	Basp.sys
Driver Version	1.4.10
Driver Date	4/12/2011

Team Properties
Displays information about the team.

Using Expert Mode

Use Expert Mode to create a team, modify a team, add a VLAN, and configure LiveLink for a Smart Load Balance and Failover and SLB (Auto-Fallback Disable) team. To create a team using the wizard, see Using the Broadcom Teaming Wizard.

To set the default Teaming Mode, select **Options** from the **Tools** menu, then select **Expert Mode** or **Wizard Mode** (the default is Wizard Mode).

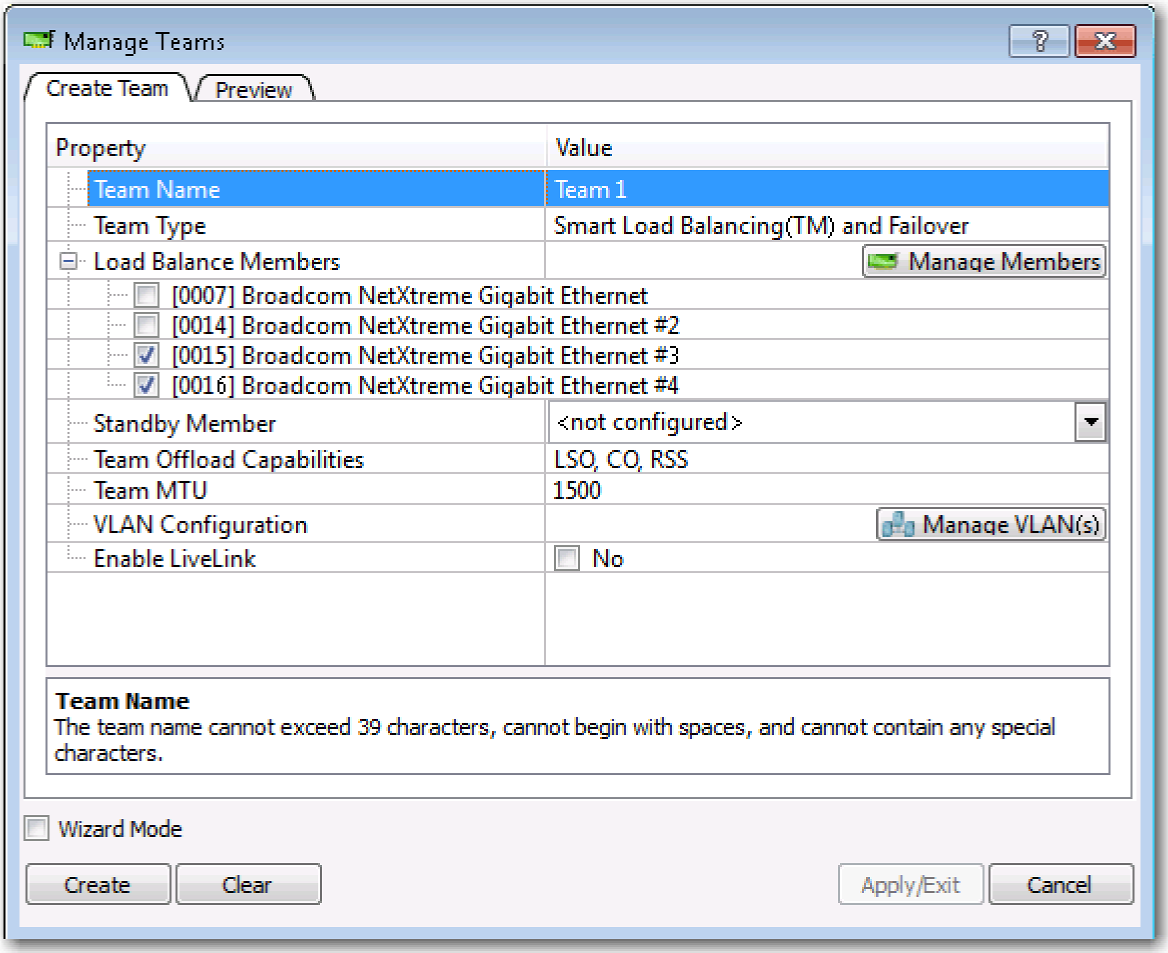
Creating a Team

Note: Enabling Dynamic Host Configuration Protocol (DHCP) is not recommended for members of an SLB type of team.

1. From the **Teams** menu, select **Create Team**, or right-click one of the devices in the “Unassigned Adapters” section and select **Create a Team**. This option is not available if there are no devices listed in the “Unassigned Adapters” sections, which means all adapters are already assigned to teams.
2. Click **Expert Mode**.

   Note: If you want to always use Expert Mode to create a team, click **Default to Expert Mode on next start**.

3. Click the **Create Team** tab.



Property	Value
Team Name	Team 1
Team Type	Smart Load Balancing(TM) and Failover
⊟ Load Balance Members	Manage Members
□ [0007] Broadcom NetXtreme Gigabit Ethernet	
□ [0014] Broadcom NetXtreme Gigabit Ethernet #2	
☑ [0015] Broadcom NetXtreme Gigabit Ethernet #3	
☑ [0016] Broadcom NetXtreme Gigabit Ethernet #4	
Standby Member	<not configured> ▾
Team Offload Capabilities	LSO, CO, RSS
Team MTU	1500
VLAN Configuration	Manage VLAN(s)
Enable LiveLink	□ No

Team Name
The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any special characters.

Note: The **Create Team** tab appears only if there are team-able adapters available.

4. Click the **Team Name** field to enter a team name.
5. Click the **Team Type** field to select a team type.
6. Assign any available adapter or adapters to the team by selecting the adapter from the **Load Balance Members** list. There must be at least one adapter selected in the **Load Balance Members** list.
7. You can assign any other available adapter to be a standby member by selecting it from the **Standby Member** list.

Note: There must be at least one Broadcom network adapter assigned to the team.

The Large Send Offload (LSO), Checksum Offload (CO), and RSS indicate if the LSO, CO, and/or RSS properties are supported for the team. The LSO, CO, and RSS properties are enabled for a team only when all of the members support and are configured for the feature.

NOTES:

- Adding a network adapter to a team where its driver is disabled may negatively affect the offloading capabilities of the team. This may have an impact on the team's performance. Therefore, it is recommended that only driver-enabled network adapters be added as members to a team.

8. Type the value for **Team MTU**.
9. Click **Create** to save the team information.
10. Repeat steps 4. through 9. to define additional teams. As teams are defined, they can be selected from the team list, but they have not yet been created. Click the **Preview** tab to view the team structure before applying the changes.
11. Click **Apply/Exit** to create all the teams you have defined and exit the Manage Teams window.
12. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

NOTES:

- The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any of the following characters: & \ / : * ? < > |
- Team names must be unique. If you attempt to use a team name more than once, an error message is displayed indicating that the name already exists.
- The maximum number of team members is 8.
- When team configuration has been correctly performed, a virtual team adapter driver is created for each configured team.
- If you disable a virtual team and later want to reenable it, you must first disable and reenable all team members before you reenable the virtual team.
- When you create Generic Trunking and Link Aggregation teams, you cannot designate a standby member. Standby members work only with Smart Load Balancing and Failover and SLB (Auto-Fallback Disable) types of teams.
- For an SLB (Auto-Fallback Disable) team, to restore traffic to the load balance members from the standby member, click the Fallback button on the Team Properties tab.
- When configuring an SLB team, although connecting team members to a hub is supported for testing, it is recommended to connect team members to a switch.
- Not all network adapters made by others are supported or fully certified for teaming.

13. Configure the team IP address.
    a. From **Control Panel**, double-click **Network Connections**.
    b. Right-click the name of the team to be configured, and then click **Properties**.
    c. On the **General** tab, click **Internet Protocol (TCP/IP)**, and then click **Properties**.
    d. Configure the IP address and any other necessary TCP/IP configuration for the team, and then click **OK** when finished.

MODIFYING A TEAM

After you have created a team, you can modify the team in the following ways:

- Change the type of team
- Change the members assigned to the team
- Add a VLAN
- Modify a VLAN (using Expert Mode)
- Remove a team or a VLAN (using Expert Mode)

To modify a team

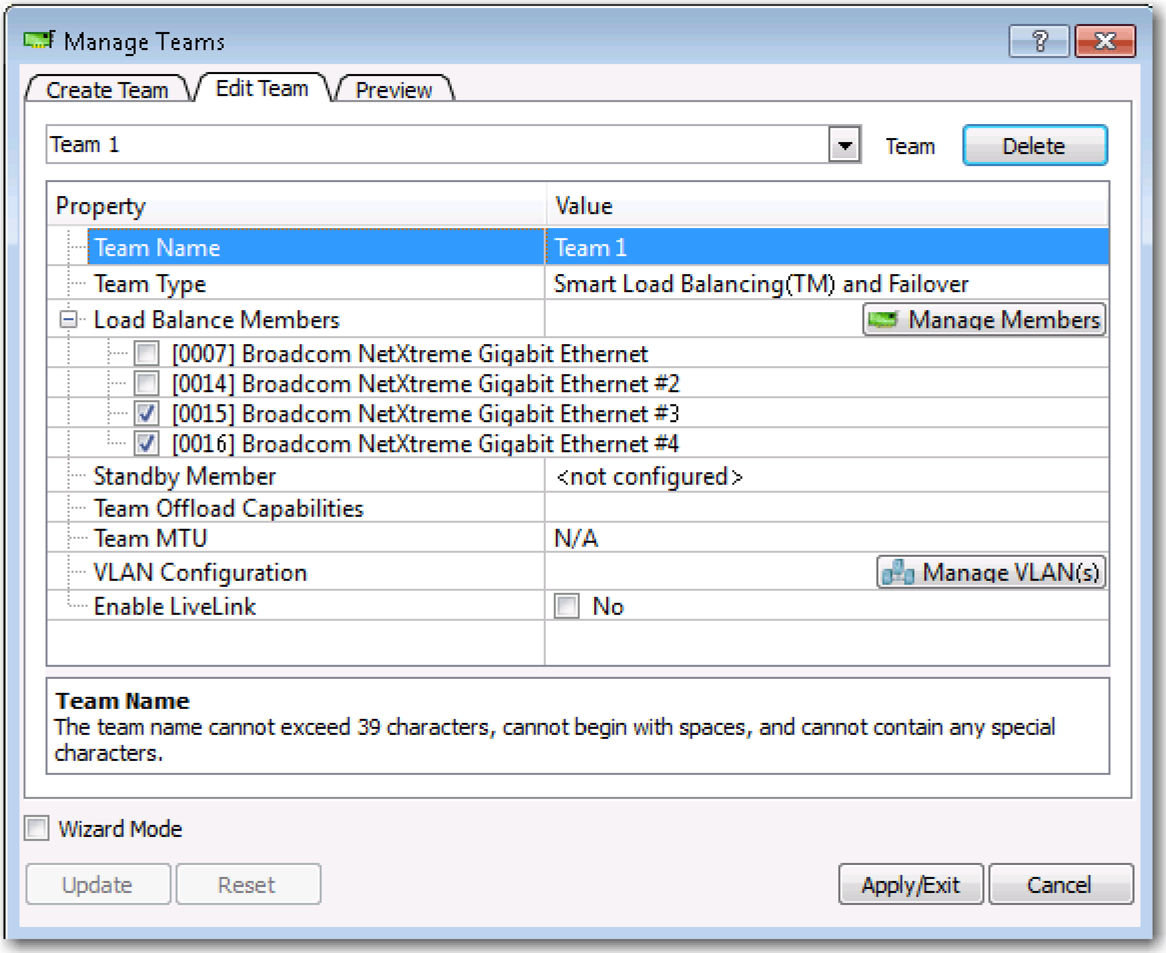
1. From the **Team** menu, click **Edit Team**, or right-click one of the teams in the list and select **Edit Team**. This option is

only available if a team has already been created and is listed in the Team Management pane.

2. The wizard Welcome screen appears. Click **Next** to continue modifying a team using the wizard or click **Expert Mode** to work in Expert Mode.

Note: The **Edit Team** tab in Expert Mode appears only if there are teams configured on the system.

3. Click the **Edit Team** tab.



Team 1

Property	Value
Team Name	Team 1
Team Type	Smart Load Balancing(TM) and Failover
Load Balance Members	Manage Members
□ [0007] Broadcom NetXtreme Gigabit Ethernet	
□ [0014] Broadcom NetXtreme Gigabit Ethernet #2	
☑ [0015] Broadcom NetXtreme Gigabit Ethernet #3	
☑ [0016] Broadcom NetXtreme Gigabit Ethernet #4	
Standby Member	<not configured>
Team Offload Capabilities	
Team MTU	N/A
VLAN Configuration	Manage VLAN(s)
Enable LiveLink	□ No

Team Name
The team name cannot exceed 39 characters, cannot begin with spaces, and cannot contain any special characters.

□ Wizard Mode

4. Make the desired changes, and then click **Update**. The changes have not yet been applied; click the **Preview** tab to view the updated team structure before applying the changes.

5. Click **Apply/Exit** to apply the updates and exit the Manage Teams window.

6. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

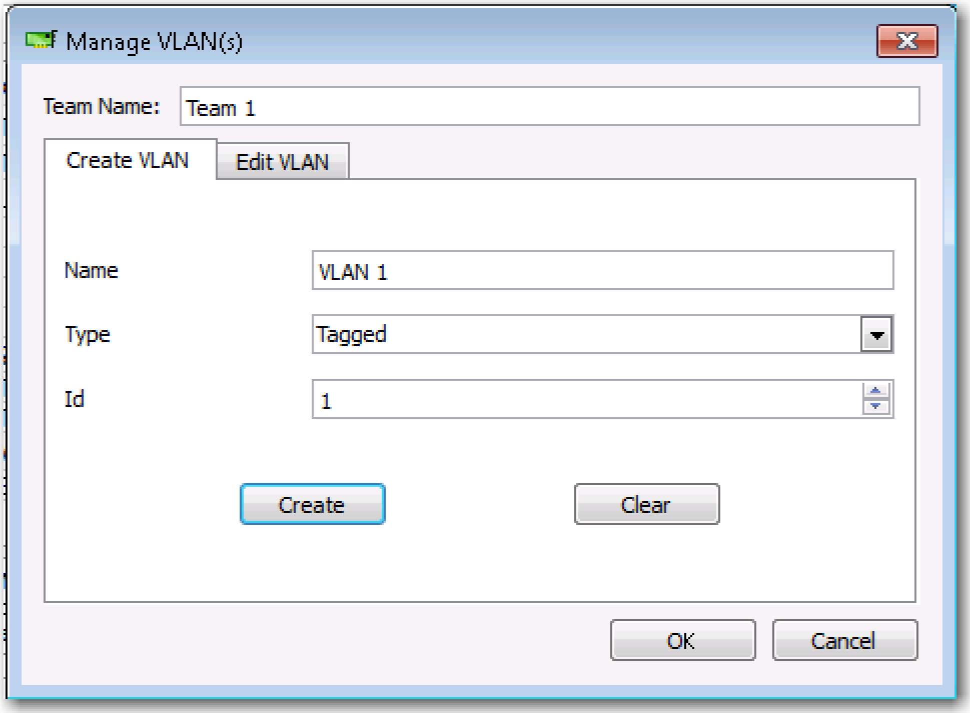
Adding a VLAN

You can add virtual LANs (VLANs) to a team. This enables you to add multiple virtual adapters that are on different subnets. The benefit of this is that your system can have one network adapter that can belong to multiple subnets. With a VLAN, you can couple the functionality of load balancing for the load balance members, and you can employ a failover adapter.

You can define up to 64 VLANs per team (63 VLANs that are tagged and 1 VLAN that is not tagged). VLANs can only be created when all teams members are Broadcom adapters. If you try to create a VLAN with a non-Broadcom adapter, an error message is displayed.

To configure a team with a VLAN

1. From the **Teams** menu, select **Add VLAN**.
2. The Welcome screen appears.
3. Click **Expert Mode**.
4. On the **Create Team** tab of the **Manage Teams** window, click **Manage VLAN(s)**.
5. Type the VLAN name, then select the type and ID.
6. Click **Create** to save the VLAN information. As VLANs are defined, they can be selected from the Team Name list, but they have not yet been created.
7. Continue this process until all VLANs are defined, then click **OK** to create them.



Manage VLAN(s)

Team Name: Team 1

Name: VLAN 1

Type: Tagged

Id: 1

8. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

Note: To maintain optimum adapter performance, your system should have 64 MB of system memory for each of the eight VLANs created per adapter.

Viewing VLAN Properties and Statistics and Running VLAN Tests

To view VLAN properties and statistics and to run VLAN tests

1. Select one of the listed VLANs.
2. Click the **Information** tab to view the properties of the VLAN adapter.

3. Click the **Statistics** tab to view the statistics for the VLAN adapter.
4. Click the **Diagnostics** tab to run a network test on the VLAN adapter.

Deleting a VLAN

The procedure below applies when you are in Expert Mode.

To delete a VLAN

1. Select the VLAN to delete.
2. From the **Teams** menu, select **Remove VLAN**.
3. Click **Apply**.
4. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.

Note: If you delete a team, any VLANs configured for that team are also deleted.

Configuring LiveLink for a Smart Load Balancing and Failover and SLB (Auto-Fallback Disable) Team

LiveLink is a feature of BASP that is available for the Smart Load Balancing (SLB) and SLB (Auto-Fallback Disable) type of teaming. The purpose of LiveLink is to detect link loss beyond the switch and to route traffic only through team members that have a live link.

Read the following notes before you attempt to configure LiveLink.

NOTES:

- Before you begin configuring LiveLink™, review the description of LiveLink. Also verify that each probe target you plan to specify is available and working. If the IP address of the probe target changes for any reason, LiveLink must be reconfigured. If the MAC address of the probe target changes for any reason, you must restart the team (see “Troubleshooting”).
- A probe target must be on the same subnet as the team, have a valid (not a broadcast, multicast, or unicast), statically-assigned IP address, and be highly available (always on).
- To ensure network connectivity to the probe target, ping the probe target from the team.
- You can specify up to four probe targets.
- The IP address assigned to either a probe target or team member cannot have a zero as the first or last octet.

To configure LiveLink

1. From the **Teams** menu, select **Edit Team**.
2. Click Expert Mode (to configure LiveLink using the Teaming Wizard, see Using the Broadcom Teaming Wizard).
3. In the Manage Members window, click the **Edit Team** tab.
4. Select **Enable LiveLink**. The LiveLink Configuration options appear below.
5. It is recommended to accept the default values for **Probe interval** (the number of seconds between each retransmission of a link packet to the probe target) and **Probe maximum retries** (the number of consecutively missed responses from a probe target before a failover is triggered). To specify different values, click the desired probe interval in the **Probe interval (seconds)** list and click the desired maximum number of probe retries in the **Probe maximum retries** list.
6. Set the **Probe VLAN ID** to correspond with the VLAN where the probe target(s) resides. This will apply the appropriate VLAN tag to the link packet based on the shared configuration of the attached switch port(s).

Note: Each LiveLink enabled team can only communicate with Probe Targets on a single VLAN. Also, VLAN ID 0 is equivalent to an untagged network.

7. Select **Probe Target 1** and type the target IP address for one or all probe targets.

Note: Only the first probe target is required. You can specify up to 3 additional probe targets to serve as backups by assigning IP addresses to the other probe targets.

8. Select one of the listed team members and type the member IP address.

Note: All of the member IP addresses must be in the same subnet as the probe targets.

9. Click **Update**. Repeat these steps for each of the other listed team members.
10. Click **Apply/Exit**.

Saving and Restoring a Configuration

To save a configuration

1. From the **File** menu, select **Team Save As**.
2. Type *the path and file name of the new configuration file*, and then click **Save** (a .bcg extension is added).

   The configuration file is a text file that can be viewed by any text editor. The file contains information about both the adapter and the team configuration.

To restore a configuration

1. From the **File** menu, select **Team Restore**.
2. Click the name of the file to be restored, and then click **Open**.

Note: If necessary, go to the folder where the file is located.

3. Click **Apply**.
4. Click **Yes** when the message is displayed indicating that the network connection will be temporarily interrupted.
5. If a configuration is already loaded, a message is displayed that asks if you want to save your current configuration. Click **Yes** to save the current configuration. Otherwise, the configuration data that is currently loaded is lost.

Note: The team may take a very long time to restore if the team is configured with many VLANs and a static IP address.

VIEWING BASP STATISTICS

The Statistics section shows performance information about the network adapters that are on a team.

To view BASP Statistics information for any team member adapter or the team as a whole, click the name of the adapter or team listed in the Team Management pane, then click the **Statistics** tab.

Click **Refresh** to get the most recent values for each statistic. Click **Reset** to change all values to zero.

Configuring With the Command Line Interface Utility

An alternate method to BACS for configuring Broadcom network adapters is with BACSCLI, which is a Broadcom utility that allows you to view information and configure network adapters using a console in either a non-interactive command line interface (CLI) mode or an interactive mode. As with BACS, BACSCLI provides information about each network adapter, and enables you to perform detailed tests, run diagnostics, view statistics, and modify property values. BACSCLI also allows you the ability to team network adapters together for load balancing and failover.

For a complete list of available commands and examples, see the BACSCLI ReadMe text file on the installation CD.

Supported Operating Systems

BACSCLI is supported on the following operating systems:

- Windows
- Windows Server
- Linux Server

For information on the latest supported OS versions, see BACSCLI_Readme.txt in your software distribution.

Installation

On a system with Broadcom NetXtreme I and NetXtreme II network adapters, BACSCLI is installed when BACS is installed with the installer.

Troubleshooting BACS

Problem: When attempting to open BACS on a Linux System, the following error message displays:

> “Another instance of the BACS client appears to be running on this system. Only one instance of the BACS client can be running at a time. If you are sure that no other BACS client is running, then a previous instance may have quit unexpectedly.”

Solution: This message displays if you try to run a second instance of BACS. If you receive this message but are certain that no instance of BACS is currently running, a previous instance of BACS may have quit unexpectedly. To clear that instance, remove the file “/dev/shm/sem.Global-BACS-{C50398EE-84A7-4bc3-9F6E-25A69603B9C0}.”

Specifications: Broadcom NetXtreme 57XX User Guide

10/100/1000BASE-T Cable Specifications

Table 1. 10/100/1000BASE-T Cable Specifications

Port Type	Connector	Media	Maximum Distance
10BASE-T	RJ-45	Category 3, 4, or 5 unshielded twisted pairs (UTP)	100m (328 ft)
100/1000BASE-T[1]	RJ-45	Category 5[2] UTP	100m (328 ft)

[1] 1000BASE-T signaling requires 4 twisted pairs of Category 5 balanced cabling, as specified in ISO/IEC 11801:1995 and ANSI/EIA/TIA-568-A (1995) and tested for additional performance using testing procedures defined in TIA/EIA TSB95.

[2] Category 5 is the minimum requirement. Category 5e and Category 6 are fully supported.

PERFORMANCE SPECIFICATIONS

Table 2. Performance Specifications

Feature	Specification
PCI Type Controllers (Single-Port BCM570X Controllers)	
PCI Clock	66 MHz maximum
PCI-X Clock	133 MHz
PCI/PCI-X Data/Address	32-bit and 64-bit
PCI-X Data Burst Transfer Rate	400 Mbit/s (32-bit bus at 100 MHz) 800 Mbit/s (64-bit bus at 100 MHz) 600 Mbit/s (32-bit bus at 100 MHz) - BCM5701/BCM5703 only 1024 Mbit/s (64-bit bus at 100 MHz) - BCM5701/BCM5703 only
PCI Data Burst Transfer Rate	132 Mbit/s (32-bit bus) 264 Mbit/s (64-bit bus) 528 Mbit/s (64-bit bus at 66 MHz)
PCI Modes	Master/slave
PCI Express™ Type Controllers (BCM57XX Controllers)	
PCI Express Interface	x1 link width
PCI Express Aggregated Bandwidth (transmit and receive)	2.5 Gbps
10/100/1000BASE-T	10/100/1000 Mbps (full-duplex)

PHYSICAL CHARACTERISTICS

Table 3. Physical Characteristics

NIC Type	Length	Width
PCI	16.6 cm (6.6 in.)	6.45 cm (2.54 in.)
PCI Express	11.2 cm (4.420 in.)	5.08 cm (2.00 in.)

POWER REQUIREMENTS

Table 4. Power Requirements

Item	**Value**
BCM5700 and BCM5701	
Operating Voltage	+5V ± 5%
Power Consumption	10W 2A @ +5VDC
BCM5703	
Operating Voltage	+3.3V ±10% for BCM95703A30 and BCM95703SA31 +5V ±5% for BCM95703A30U and BCM95703SA31U
Power Consumption	4W 1.2A@ +3.3V for BCM95703A30
BCM5721 and BCM5751	
Operating voltage	+3.3V ± 10%
Power Consumption	2.84W 860 mA @ +3.3VDC
BCM5722	
Operating voltage	+3.3V ± 10%
Power Consumption	1.41W 427 mA @ +3.3VDC
BCM5705	
Operating Voltage	+3.3V ± 10%
Power Consumption	1.13W maximum

ENVIRONMENTAL SPECIFICATIONS

Table 5. Environmental Specifications

Condition	Operating Specification	Storage Specification
Temperature	0°C to 55°C (+32°F to +131°F)	–40°C to +85°C (–40°F to +185°F)
Relative Humidity	5% to 85% (non-condensing) 40°C, 16-hour dwells at extremes	5% to 95% (non-condensing) 10°C/hour
Altitude	Up to 10,000 ft.	Up to 35,000 ft.
Shock	10g, 1/2 sine wave, 11 ms	60g, 1/2 sine wave, 11 ms
Vibration, peak-to-peak displacement	0.005 in. max (5 Hz to 32 Hz)	0.1 in. max (5 Hz to 17 Hz)
Vibration, peak acceleration	0.25g (5 Hz to 500 Hz) (Sweep Rate = 1 octave/min.)	0.25g (5 Hz to 500 Hz) (Sweep Rate = 1 octave/min.)

Regulatory Information: Broadcom NetXtreme 57XX User Guide

FCC Class B Notice

Broadcom NetXtreme Gigabit Ethernet Controller
The equipment complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: 1) The device may not cause harmful interference, and 2) This equipment must accept any interference received, including interference that may cause undesired operation.

The equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. The equipment generates, uses and can radiate radio-frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If the equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and the receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for assistance.

Do not make mechanical or electrical modifications to the equipment.

NOTE: If you change or modify the adapter without permission of Broadcom, you may void your authority to operate the equipment.

Broadcom Corporation
190 Mathilda Place
Sunnyvale, California 94086 USA

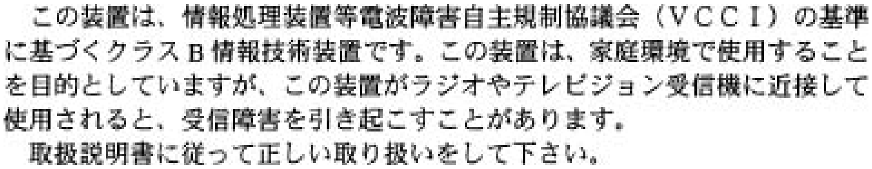
VCCI Class B Notice

The equipment is a Class B product based on the standard of the Voluntary Control Council for Interference from Information Technology Equipment (VCCI). If used near a radio or television receiver in a domestic environment, it may cause radio interference. Install and use the equipment according to the instruction manual.

⚠

CAUTION! The potential exists for this equipment to become impaired in the presence of conducted radio frequency energy between the frequency range of 59–66 MHz. Normal operation will return upon removal of the RF energy source.

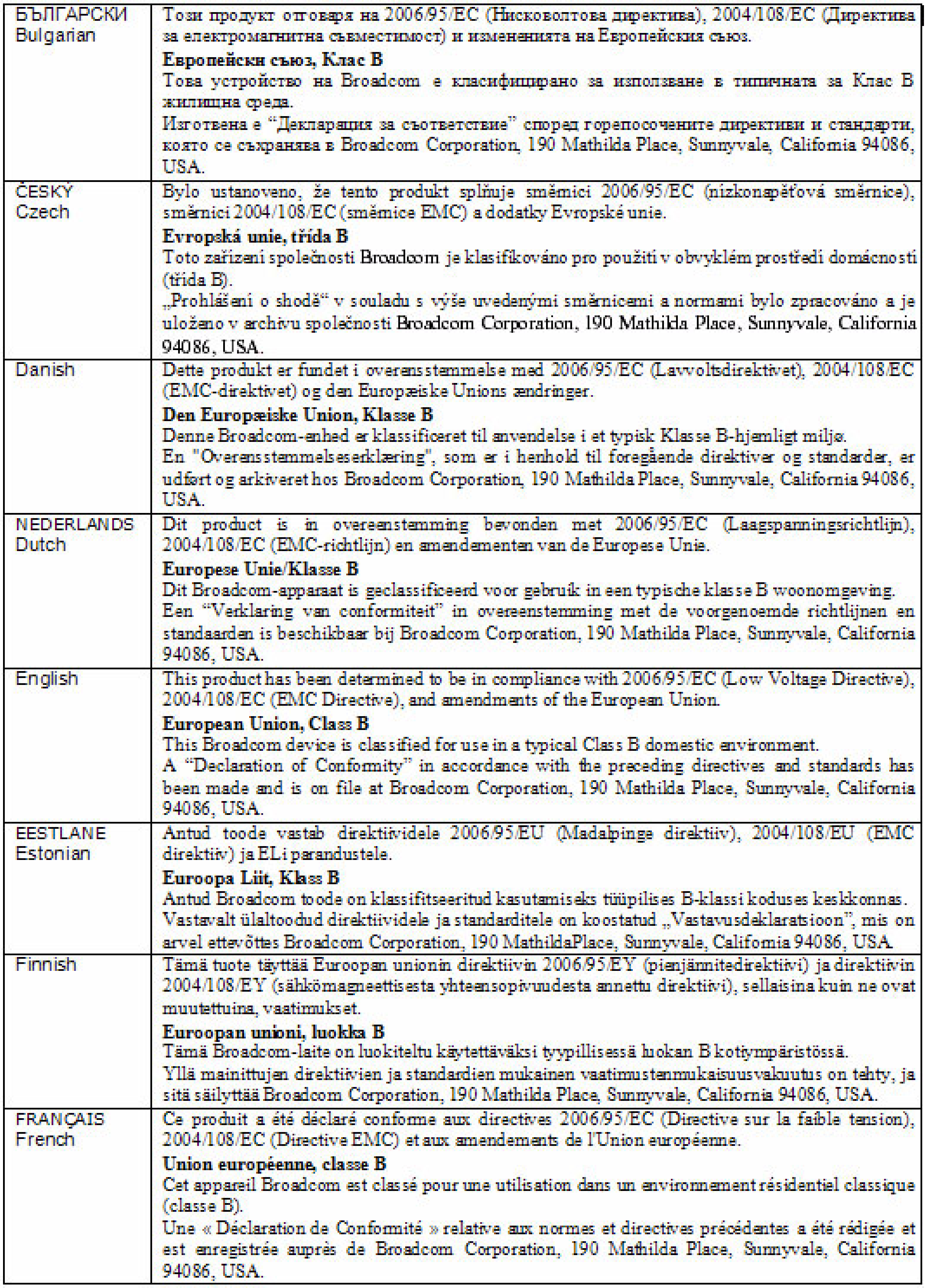
VCCI Class B Statement (Japan)



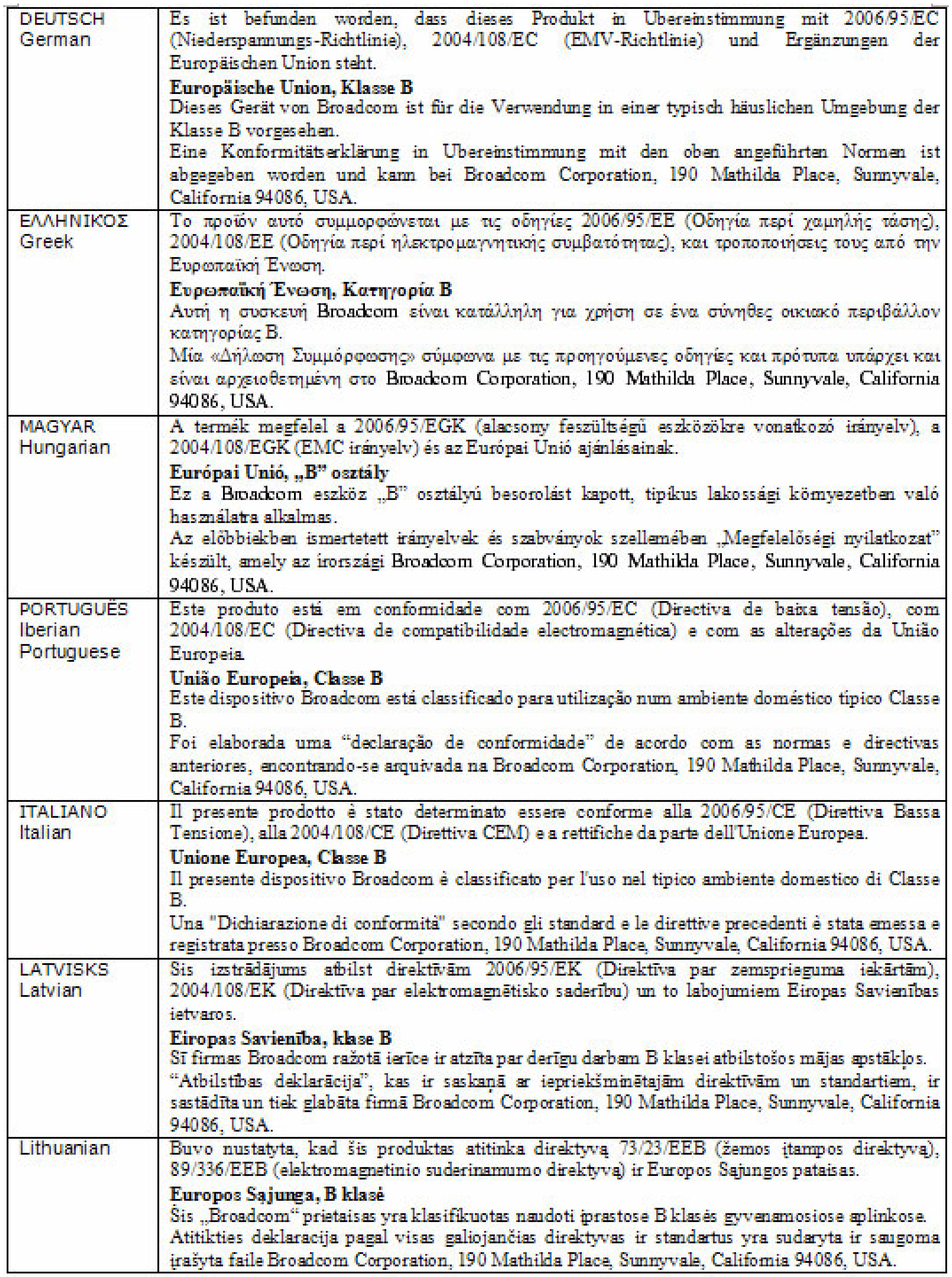
　この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスＢ情報技術装置です。この装置は、家庭環境で使用することを目的としていますが、この装置がラジオやテレビジョン受信機に近接して使用されると、受信障害を引き起こすことがあります。

　取扱説明書に従って正しい取り扱いをして下さい。

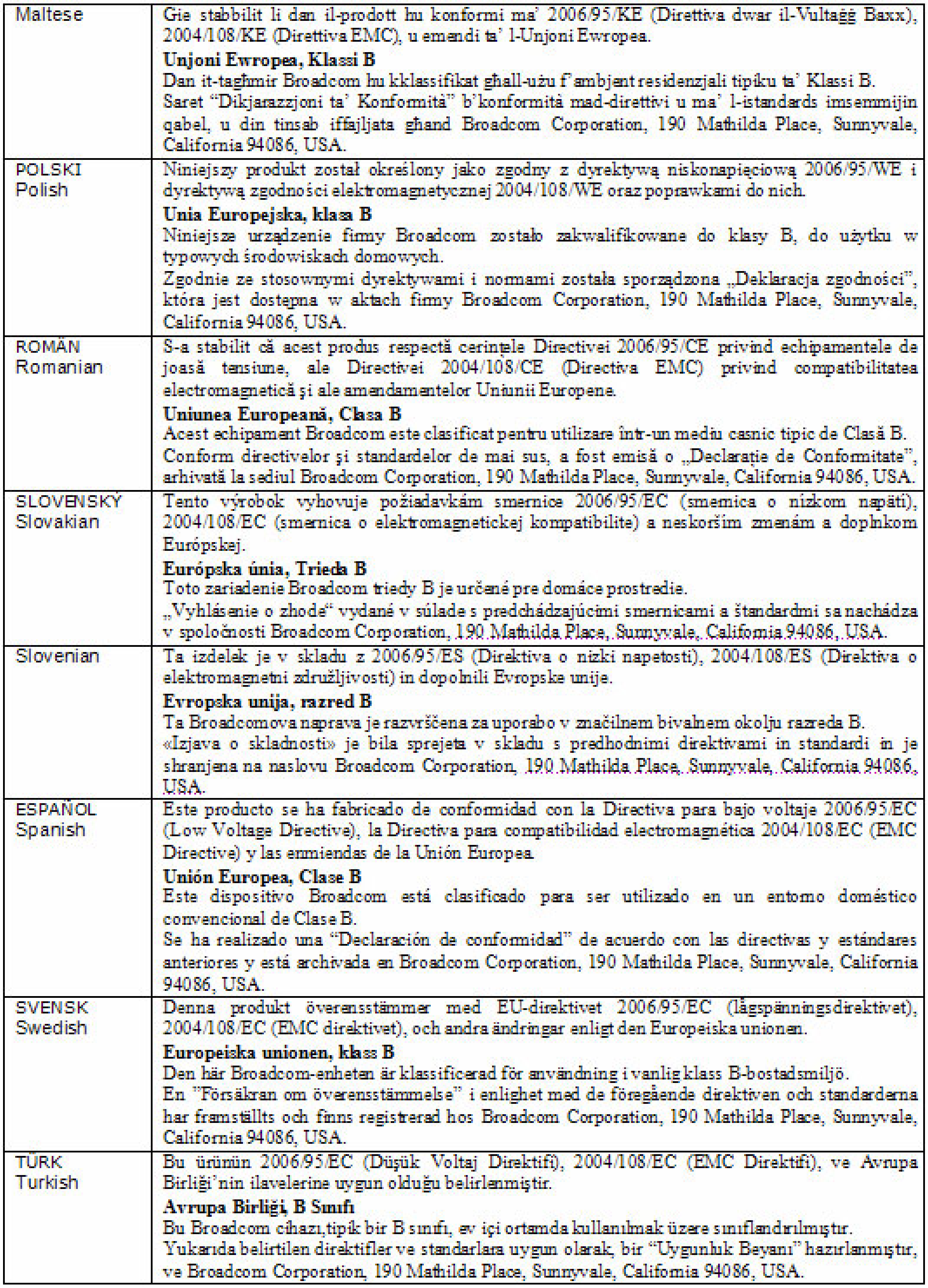
CE Notice



БЪЛГАРСКИ Bulgarian	Този продукт отговаря на 2006/95/EC (Нисковолтова директива), 2004/108/EC (Директива за електромагнитна съвместимост) и измененията на Европейския съюз. **Европейски съюз, Клас B** Това устройство на Broadcom е класифицирано за използване в типичната за Клас B жилищна среда. Изготвена е "Декларация за съответствие" според горепосочените директиви и стандарти, която се съхранява в Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ČESKÝ Czech	Bylo ustanoveno, že tento produkt splňuje směrnici 2006/95/EC (nízkonapěťová směrnice), směrnici 2004/108/EC (směrnice EMC) a dodatky Evropské unie. **Evropská unie, třída B** Toto zařízení společnosti Broadcom je klasifikováno pro použití v obvyklém prostředí domácnosti (třída B). „Prohlášení o shodě" v souladu s výše uvedenými směrnicemi a normami bylo zpracováno a je uloženo v archivu společnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
Danish	Dette produkt er fundet i overensstemmelse med 2006/95/EC (Lavvoltsdirektivet), 2004/108/EC (EMC-direktivet) og den Europæiske Unions ændringer. **Den Europæiske Union, Klasse B** Denne Broadcom-enhed er klassificeret til anvendelse i et typisk Klasse B-hjemligt miljø. En "Overensstemmelseserklæring", som er i henhold til foregående direktiver og standarder, er udført og arkiveret hos Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
NEDERLANDS Dutch	Dit product is in overeenstemming bevonden met 2006/95/EC (Laagspanningsrichtlijn), 2004/108/EC (EMC-richtlijn) en amendementen van de Europese Unie. **Europese Unie/Klasse B** Dit Broadcom-apparaat is geclassificeerd voor gebruik in een typische klasse B woonomgeving. Een "Verklaring van conformiteit" in overeenstemming met de voorgenoemde richtlijnen en standaarden is beschikbaar bij Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
English	This product has been determined to be in compliance with 2006/95/EC (Low Voltage Directive), 2004/108/EC (EMC Directive), and amendments of the European Union. **European Union, Class B** This Broadcom device is classified for use in a typical Class B domestic environment. A "Declaration of Conformity" in accordance with the preceding directives and standards has been made and is on file at Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
EESTLANE Estonian	Antud toode vastab direktiividele 2006/95/EU (Madalpinge direktiiv), 2004/108/EU (EMC direktiiv) ja ELi parandustele. **Euroopa Liit, Klass B** Antud Broadcom toode on klassifitseeritud kasutamiseks tüüpilises B-klassi koduses keskkonnas. Vastavalt ülaltoodud direktiividele ja standarditele on koostatud „Vastavusdeklaratsioon", mis on arvel ettevõttes Broadcom Corporation, 190 MathildaPlace, Sunnyvale, California 94086, USA.
Finnish	Tämä tuote täyttää Euroopan unionin direktiivin 2006/95/EY (pienjännitedirektiivi) ja direktiivin 2004/108/EY (sähkömagneettisesta yhteensopivuudesta annettu direktiivi), sellaisina kuin ne ovat muutettuina, vaatimukset. **Euroopan unioni, luokka B** Tämä Broadcom-laite on luokiteltu käytettäväksi tyypillisessä luokan B kotiympäristössä. Yllä mainittujen direktiivien ja standardien mukainen vaatimustenmukaisuusvakuutus on tehty, ja sitä säilyttää Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
FRANÇAIS French	Ce produit a été déclaré conforme aux directives 2006/95/EC (Directive sur la faible tension), 2004/108/EC (Directive EMC) et aux amendements de l'Union européenne. **Union européenne, classe B** Cet appareil Broadcom est classé pour une utilisation dans un environnement résidentiel classique (classe B). Une « Déclaration de Conformité » relative aux normes et directives précédentes a été rédigée et est enregistrée auprès de Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.



DEUTSCH German	Es ist befunden worden, dass dieses Produkt in Ubereinstimmung mit 2006/95/EC (Niederspannungs-Richtlinie), 2004/108/EC (EMV-Richtlinie) und Ergänzungen der Europäischen Union steht. **Europäische Union, Klasse B** Dieses Gerät von Broadcom ist für die Verwendung in einer typisch häuslichen Umgebung der Klasse B vorgesehen. Eine Konformitätserklärung in Ubereinstimmung mit den oben angeführten Normen ist abgegeben worden und kann bei Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ΕΛΛΗΝΙΚΟΣ Greek	Το προϊόν αυτό συμμορφώνεται με τις οδηγίες 2006/95/ΕΕ (Οδηγία περί χαμηλής τάσης), 2004/108/ΕΕ (Οδηγία περί ηλεκτρομαγνητικής συμβατότητας), και τροποποιήσεις τους από την Ευρωπαϊκή Ένωση. **Ευρωπαϊκή Ένωση, Κατηγορία B** Αυτή η συσκευή Broadcom είναι κατάλληλη για χρήση σε ένα σύνηθες οικιακό περιβάλλον κατηγορίας B. Μία «Δήλωση Συμμόρφωσης» σύμφωνα με τις προηγούμενες οδηγίες και πρότυπα υπάρχει και είναι αρχειοθετημένη στο Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
MAGYAR Hungarian	A termék megfelel a 2006/95/EGK (alacsony feszültségű eszközökre vonatkozó irányelv), a 2004/108/EGK (EMC irányelv) és az Európai Unió ajánlásainak. **Európai Unió, „B" osztály** Ez a Broadcom eszköz „B" osztályú besorolást kapott, tipikus lakossági környezetben való használatra alkalmas. Az elöbbiekben ismertetett irányelvek és szabványok szellemében „Megfelelőségi nyilatkozat" készült, amely az irországi Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
PORTUGUËS Iberian Portuguese	Este produto está em conformidade com 2006/95/EC (Directiva de baixa tensão), com 2004/108/EC (Directiva de compatibilidade electromagnética) e com as alterações da União Europeia **União Europeia, Classe B** Este dispositivo Broadcom está classificado para utilização num ambiente doméstico típico Classe B. Foi elaborada uma "declaração de conformidade" de acordo com as normas e directivas anteriores, encontrando-se arquivada na Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ITALIANO Italian	Il presente prodotto è stato determinato essere conforme alla 2006/95/CE (Direttiva Bassa Tensione), alla 2004/108/CE (Direttiva CEM) e a rettifiche da parte dell'Unione Europea. **Unione Europea, Classe B** Il presente dispositivo Broadcom è classificato per l'uso nel tipico ambiente domestico di Classe B. Una "Dichiarazione di conformità" secondo gli standard e le direttive precedenti è stata emessa e registrata presso Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
LATVISKS Latvian	Sis izstrādājums atbilst direktīvām 2006/95/EK (Direktīva par zemsprieguma iekārtām), 2004/108/EK (Direktīva par elektromagnētisko saderību) un to labojumiem Eiropas Savienības ietvaros. **Eiropas Savienība, klase B** Sī firmas Broadcom ražotā ierīce ir atzīta par derīgu darbam B klasei atbilstošos mājas apstākļos. "Atbilstības deklarācija", kas ir saskaņā ar iepriekšminētajām direktīvām un standartiem, ir sastādīta un tiek glabāta firmā Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
Lithuanian	Buvo nustatyta, kad šis produktas atitinka direktyvą 73/23/EEB (žemos įtampos direktyvą), 89/336/EEB (elektromagnetinio suderinamumo direktyvą) ir Europos Sąjungos pataisas. **Europos Sąjunga, B klasė** Šis „Broadcom" prietaisas yra klasifikuotas naudoti įprastose B klasės gyvenamosiose aplinkose. Atitikties deklaracija pagal visas galiojančias direktyvas ir standartus yra sudaryta ir saugoma įrašyta faile Broadcom Corporation, 190 Mathilda Place, Sunnyvale, Califomia 94086, USA.



Maltese	Gie stabbilit li dan il-prodott hu konformi ma' 2006/95/KE (Direttiva dwar il-Vultaġġ Baxx), 2004/108/KE (Direttiva EMC), u emendi ta' l-Unjoni Ewropea. **Unjoni Ewropea, Klassi B** Dan it-tagħmir Broadcom hu kklassifikat għall-użu f'ambjent residenzjali tipiku ta' Klassi B. Saret "Dikjarazzjoni ta' Konformità" b'konformità mad-direttivi u ma' l-istandards imsemmijin qabel, u din tinsab iffajljata għand Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
POLSKI Polish	Niniejszy produkt został określony jako zgodny z dyrektywą niskonapięciową 2006/95/WE i dyrektywą zgodności elektromagnetycznej 2004/108/WE oraz poprawkami do nich. **Unia Europejska, klasa B** Niniejsze urządzenie firmy Broadcom zostało zakwalifikowane do klasy B, do użytku w typowych środowiskach domowych. Zgodnie ze stosownymi dyrektywami i normami została sporządzona „Deklaracja zgodności", która jest dostepna w aktach firmy Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ROMÂN Romanian	S-a stabilit că acest produs respectă cerințele Directivei 2006/95/CE privind echipamentele de joasă tensiune, ale Directivei 2004/108/CE (Directiva EMC) privind compatibilitatea electromagnetică şi ale amendamentelor Uniunii Europene. **Uniunea Europeană, Clasa B** Acest echipament Broadcom este clasificat pentru utilizare într-un mediu casnic tipic de Clasă B. Conform directivelor şi standardelor de mai sus, a fost emisă o „Declarație de Conformitate", arhivată la sediul Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
SLOVENSKÝ Slovakian	Tento výrobok vyhovuje požiadavkám smernice 2006/95/EC (smernica o nízkom napätí), 2004/108/EC (smernica o elektromagnetickej kompatibilite) a neskorším zmenám a doplnkom Európskej. **Európska únia, Trieda B** Toto zariadenie Broadcom triedy B je určené pre domáce prostredie. „Vyhlásenie o zhode" vydané v súlade s predchádzajúcimi smernicami a štandardmi sa nachádza v spoločnosti Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
Slovenian	Ta izdelek je v skladu z 2006/95/ES (Direktiva o nizki napetosti), 2004/108/ES (Direktiva o elektromagnetni združljivosti) in dopolnili Evropske unije. **Evropska unija, razred B** Ta Broadcomova naprava je razvrščena za uporabo v značilnem bivalnem okolju razreda B. «Izjava o skladnosti» je bila sprejeta v skladu s predhodnimi direktivami in standardi in je shranjena na naslovu Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
ESPAÑOL Spanish	Este producto se ha fabricado de conformidad con la Directiva para bajo voltaje 2006/95/EC (Low Voltage Directive), la Directiva para compatibilidad electromagnética 2004/108/EC (EMC Directive) y las enmiendas de la Unión Europea. **Unión Europea, Clase B** Este dispositivo Broadcom está clasificado para ser utilizado en un entorno doméstico convencional de Clase B. Se ha realizado una "Declaración de conformidad" de acuerdo con las directivas y estándares anteriores y está archivada en Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
SVENSK Swedish	Denna produkt överensstämmer med EU-direktivet 2006/95/EC (lågspänningsdirektivet), 2004/108/EC (EMC direktivet), och andra ändringar enligt den Europeiska unionen. **Europeiska unionen, klass B** Den här Broadcom-enheten är klassificerad för användning i vanlig klass B-bostadsmiljö. En "Försäkran om överensstämmelse" i enlighet med de föregående direktiven och standarderna har framställts och finns registrerad hos Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.
TÜRK Turkish	Bu ürünün 2006/95/EC (Düşük Voltaj Direktifi), 2004/108/EC (EMC Direktifi), ve Avrupa Birliği'nin ilavelerine uygun olduğu belirlenmiştir. **Avrupa Birliği, B Sınıfı** Bu Broadcom cihazı,tipik bir B sınıfı, ev içi ortamda kullanılmak üzere sınıflandırılmıştır. Yukarıda belirtilen direktifler ve standarlara uygun olarak, bir "Uygunluk Beyanı" hazırlanmıştır, ve Broadcom Corporation, 190 Mathilda Place, Sunnyvale, California 94086, USA.

Canadian Regulatory Information (Canada Only)

Industry Canada, Class B

This Class B digital apparatus complies with Canadian ICES-003.

Notice: The Industry Canada regulations provide that changes or modifications not expressly approved by Broadcom could void your authority to operate this equipment.

Industry Canada, classe B

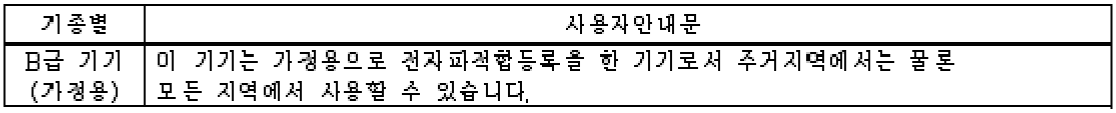
Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.

Avis : Dans le cadre des réglementations d'Industry Canada, vos droits d'utilisation de cet équipement peuvent être annulés si des changements ou modifications non expressément approuvés par Broadcom y sont apportés.

MIC Notice (Republic of Korea Only)

B CLASS Device

Broadcom NetXtreme Gigabit Ethernet Controller



기종별	사용자안내문
B급 기기 (가정용)	이 기기는 가정용으로 전자파적합등록을 한 기기로서 주거지역에서는 물론 모든 지역에서 사용할 수 있습니다.

Note that this device has been approved for non-business purposes and may be used in any environment, including residential areas.

User Diagnostics: Broadcom Broadcom NetXtreme 57XX User Guide

INTRODUCTION

Broadcom NetXtreme User Diagnostics is an MS-DOS based application that runs a series of diagnostic tests (see Table 1: “MS-DOS Command Prompt Mode Command Options”) on the Broadcom NetXtreme Gigabit Ethernet adapters in your system. Broadcom NetXtreme User Diagnostics also allows you to update device firmware and to view and change settings for available adapter properties. Broadcom NetXtreme User Diagnostics can be run in either of the following modes:

- MS-DOS Command Prompt mode
- Broadcom Command Line Interface (CLI) mode

In either mode, you can view the version of the adapter software and specify which adapter to test and which tests to perform. The MS-DOS Command Prompt mode is useful for viewing and changing the settings for available properties, updating and loading device firmware, viewing the version of and printing the error log (if any) to a file. The Broadcom CLI mode is useful for enabling/disabling available properties and enabling/disabling/selecting and setting the speed and duplex mode of available protocols.

To run Broadcom NetXtreme User Diagnostics, create an MS-DOS 6.22 bootable disk containing the B57udiag.exe file. Next, start the system with the boot disk in drive A. See either Running in MS-DOS Command Prompt Mode or Running in Broadcom Command Line Interface Mode for further instructions.

SYSTEM REQUIREMENTS

Operating System: MS-DOS 6.22

Software: B57udiag.exe

Running Broadcom NetXtreme User Diagnostics

Running in MS-DOS Command Prompt Mode

At the MS-DOS prompt, type b57udiag using the command options as shown in Table 1.

NOTE: In MS-DOS Command Prompt mode, you must include b57udiag at the beginning of the command string each time you type a command.

Table 1: MS-DOS Command Prompt Mode Command Options

Command Options	*Description*
b57udiag	Performs all of the tests on all of the Broadcom NetXtreme Gigabit Ethernet adapters in your system.
b57udiag -c <num>	Specifies the adapter to test, or the adapter on which to update the firmware or to view or change the settings for available properties.
b57udiag -cmd	Changes to the Broadcom CLI mode.
b57udiag -w <value>	Enables/disables the Wake on LAN (WOL) property. 1 = Enable 0 = Disable
b57udiag -mba <value>	Enables/disables Multi-Boot Agent (MBA) protocol. 1 = Enable 0 = Disable
b57udiag -mbap <value>	Selects the specific MBA protocol. 0 = Preboot Execution Environment (PXE) 1 = Remote Program Load (RPL) 2 = Bootstrap Protocol (BOOTP)
b57udiag -mbas <value>	Selects the MBA speed and duplex mode. 0 = Auto 1 = 10 Mbps speed, half-duplex operation 2 = 10 Mbps speed, full-duplex operation 3 = 100 Mbps speed, half-duplex operation 4 = 100 Mbps speed, full-duplex operation 6 = 1000 Mbps speed, full-duplex (fiber)

b57udiag -firm <file>	Updates the EEPROM of the selected adapter based on the match between the existing image file name and the new image <file name>.
	Examples:
	`b57udiag -firm ee5751c3.40a`
	`b57udiag -firm ee5721c3.40a`

b57udiag -firmall <file>	Updates the EEPROM of all of the adapters based on the <file name> image match.
b57udiag -ver	Displays the version of the software/eeprom.bin file.

Table 1: MS-DOS Command Prompt Mode Command Options (Cont.)

Command Options	Description
b57udiag -pxe <file>	Loads the Preboot Execution Environment (PXE) firmware from a file. **Example:** `b57udiag -pxe b57mmba.nic` **Note:** This command should be used only for add-in adapters. For LOM adapters, the PXE firmware is loaded automatically during startup.
b57udiag -elog <file>	Prints the error log to a file.

b57udiag -pipmi <file>	Loads the Intelligent Platform Management Interface (IPMI) from a file.
	`b57udiag -pipmi pt5721c6.10`
	`b57udiag -pipmi pt5704c2.36`
	`b57udiag -pipmi pt5704s2.36`
	Use the file that is appropriate for the type of hardware interface (copper or fiber). For example, the pt5704c2.36 file should be used for copper, and the pt5704s2.36 file should be used for fiber.

b57udiag -ipmi <value>	Enables/disables IPMI. 1 = Enable 0 = Disable
b57udiag -help	Displays this table of MS-DOS Command Prompt Mode Command Options.

RUNNING IN BROADCOM COMMAND LINE INTERFACE MODE

At the MS-DOS prompt, type `b57udiag -cmd`, and use the command options as shown in Table 2

NOTE: The values for settings are in decimal notation unless otherwise indicated.

Table 2: Broadcom Command Line Interface (CLI) Mode Commands

Command	Description
upgfrm	Updates the PXE or Boot Code from a file
dir	Displays the file directory in NVRAM. Example:

```
Entry  Type            SRAM Addr EEP Offset  Length    Execute   Version
       Boot Code       08003000  00000200    000011B0  CPUA(2)   5721-v6.17
0      PXE             00010000  000013Bo    0000C854  NO        7.0.1
1      AdvancedFw CFG  00000000  0001027C    000001D4  NO        IPMIc V2.15
2      AdvancedFw CPUB C0034000  00010450    00002654  NO        IPMIc V2.15
3      AdvancedFw CPUA 08000000  00012AA4    000035B4  NO        IPMIc V2.15
4      AdvancedFwINIT  C0034000  00016058    00001A94  CPUB      IPMIc V2.15
```

setwol	Enables/disables the Wake on LAN (WOL) property. `setwol e` = Enable WOL `setwol d` = Disable WOL

Table 2: Broadcom Command Line Interface (CLI) Mode Commands (Cont.)

Command	*Description*
setpxe	Enables/disables Preboot Exchange Environment (PXE) and sets PXE speed `setpxe e` = Enable PXE `setpxe d` = Disable PXE `setpxe s 0` = Auto (Default) `setpxe s 1` = 10 Mbps speed, half-duplex operation `setpxe s 2` = 10 Mbps speed, full-duplex operation `setpxe s 3` = 100 Mbps speed, half-duplex operation `setpxe s 4` = 100 Mbps speed, full-duplex operation
setasf	Enables/disables Alert Standard Format (ASF) Do not use. Alert Standard Format (ASF) is not for system platforms.
setmba	Enables/disables Multi Boot Agent (MBA) and selects the MBA protocol `setmba d` = Disable MBA `setmba e 0` = Enable Preboot Execution Environment (PXE) MBA (default) `setmba e 1` = Enable Remote Program Load (RPL) MBA `setmba e 2` = Enable Boot Protocol (BootP) MBA `setmba s 0` = Auto speed and duplex (default) `setmba s 1` = 10 Mbps speed, half-duplex operation `setmba s 2` = 10 Mbps speed, full-duplex operation `setmba s 3` = 100 Mbps speed, half-duplex operation `setmba s 4` = 100 Mbps speed, full-duplex operation `setmba s 6` = 1000 Mbps full-duplex (fiber)
setipmi	Enables/disables Intelligent Platform Management Interface (IPMI) `setipmi e` = Enable IPMI `setipmi d` = Disable IPMI
nictest	Runs the specified diagnostic tests Specify which individual test(s) within a group or which group(s) of tests to run by including the test designation or group designation in the command string, as shown in the examples below: `nictest abcd` = Run all tests `nictest b` = Run all tests in group B `nictest a3b1` = Run tests A3 and B1 only `nictest a124b2` = Run tests A1, A2, A4, and B2
exit	Changes from the Broadcom CLI mode to the MS-DOS command prompt mode
device	Selects the device (adapter) `device <n>` = Device number in hexadecimal notation (default = 00000000) `device r` = Remove all current Broadcom adapters and rescan available adapters `device s` = Silent mode (adapters are not displayed)
version	Displays the version of the adapter software
help	Displays this list of commands
reset	Resets the Broadcom NetXtreme Gigabit Ethernet chip `reset c` = Simulate a cold reset `reset w` = Wait for firmware signature `reset t` = Display the time from reset to firmware invert signature
cls	Clears the screen

Table 2: Broadcom Command Line Interface (CLI) Mode Commands (Cont.)

Command	*Description*
asfprg	Loads Alert Standard Format (ASF) into NVRAM Do not use. Alert Standard Format (ASF) is not for system platforms.

DIAGNOSTIC TEST DESCRIPTIONS

The diagnostic tests are divided into 4 groups: Register Tests (Group A), Memory Tests (Group B), Miscellaneous Tests (Group C), and Driver Associated Tests (Group D). The diagnostic tests are listed and described in Table 3.

Table 3: Diagnostic Tests

Test		*Description*
Number	*Name*	
Group A: Register Tests		
A1	Indirect Register	This test uses an indirect addressing method to write an increment of data to the MAC hash register table and read back data for verification. The memory read/write is done 100 times while incrementing test data.

A2	Control Register	Each register specified in the configuration content defines the read-only bit and the read/write bits. The test writes 0s and 1s to the test bits to ensure the read-only bits are not changed, and that read/write bits are changed.
		This test attempts to read the register configuration file (Ctrlreg.txt) for the register definitions. If the file does not exist, a default register offset and mask bits are used.
		`Offset       Read-Only Mask   Read/Write Mask`
		`0x00000400   0x00000000       0x007FFF8C`
		`0x00000404   0x03800107       0x00000000`

A3	Interrupt	This test verifies the interrupt functionality. It enables an interrupt and waits 500 ms for the interrupt to occur and reports an error if it cannot generate the interrupt.
A4	Built-In Self-Test	This is the hardware built-in self-test (BIST).
A5	PCI Cfg Register	This test verifies the access integrity of the PCI configuration registers.
Group B: Memory Tests		

Table 3: Diagnostic Tests (Cont.)

Test		Description
Number	**Name**	
B1	Scratch Pad	This test tests the onboard scratchpad SRAM. The following tests are performed: **Address Test.** This test writes each address with a unique increment of data and reads back data to ensure data is correct. After filling the entire address with the unique data, the program reads back the data again to ensure that the data is still correct. **Walking bit.** For each address, data one is written and read back for testing. Then it shifts the data left one bit, so the data becomes two and repeats the same test. It repeats the test 32 times until the test bit is shifted out of the test address. The same test is repeated for entire test range. **Pseudo-Random Data.** A precalculated pseudo-random data set is used to write unique data to each test RAM. After passing the test, the program reads back the data one more time to ensure that the data is still correct. **Data Read/Write Test:** This test writes test data to the SRAM and reads it back to ensure that the data is correct. The test data used is 0x00000000, 0xFFFFFFFF, 0xAA55AA55, and 0x55AA55AA. **Alternate Data Pattern Test.** This test writes test data into the SRAM, writes complement test data to the next address, and reads back both to ensure the data is correct. After the test, the program reads back data one more time to ensure that the data is still correct. The test data used is 0x00000000, 0xFFFFFFFF, 0xAA55AA55, and 0x55AA55AA.
B2	BD SRAM	This test tests the Buffer Descriptor (BD) SRAM. This test performs in the same way as the Scratch Pad Test described in B1.
B3	DMA SRAM	This test tests the direct memory access (DMA) SRAM by performing the Scratch Pad Test described in test B1.
B4	MBUF SRAM	This test tests the memory access buffer (MBUF) SRAM by performing the Scratch Pad Test described in test B1.

Table 3: Diagnostic Tests (Cont.)

Test		Description
Number	**Name**	
B5	MBUF SRAM via DMA	This test uses 8 data test patterns. A 0x1000-sized data buffer is used for this test. Before each pattern test, the buffer is initialized and filled with the test pattern. It then performs a 0x1000-sized transmit DMA from the host buffer to the adapter MBUF memory. The test verifies the data integrity in the adapter MBUF memory against the host memory and repeats the DMA for the entire MBUF buffer. Then, the test performs a receive DMA from the adapter to the host. The 0x1000-byte test buffer is cleared to 0 before each receive DMA. After the test verifies the integrity of the data, the test is repeated for the entire MBUF SRAM range. The 8 test patterns are described below. **Test Pattern Description** 16 00s and 16 FF's Fills the entire host DMA buffer with 16 bytes of 00s and then 16 bytes of FF's. 16 FF's and 16 00s Fills the entire host DMA buffer with 16 bytes of FF's and then 16 bytes of 00s. 32 00s and 32 FF's Fills the entire host DMA buffer with 32 bytes of 00s and then 32 bytes of FF's. 32 FF's and 32 00s Fills the entire host DMA buffer with 32 bytes of FF's and then 32 bytes of 00s. 00000000 Fills the entire host DMA buffer with all 00s. FFFFFFFF Fills the entire host DMA buffer with all FF's. AA55AA55 Fills the entire host DMA buffer with data 0xAA55AA55. 55AA55AA Fills the entire host DMA buffer with data 0x55AA55AA.
B7	CPU GPR	This test tests the CPU General Purpose registers and performs in the same way as the Scratch Pad Test (B1) over 3 different voltages (1.1V, 1.2V, and 1.3V).
Group C: Miscellaneous Tests		
C1	NVRAM	Incremental test data is used in the electrically erasable programmable read-only memory (EEPROM) test. The test fills the test range with test data and reads the data back to verify the content. Afterwards, the test fills the test range with 0s to clear the memory.
C2	CPU	This test opens the Cpu.bin file. If the file exists and content is good, the test loads code to the RX CPU and TX CPU and verifies the CPU execution.
C3	DMA	This test tests both high-priority direct memory access (DMA) and low-priority DMA. The test moves data from the host memory to the adapter SRAM and verifies the data. The test then moves data back to the host memory to again verify the data.

Table 3: Diagnostic Tests (Cont.)

Test		Description
Number	**Name**	

C4	MII	The medium independent interface (MII) test function is identical to that of the Control Register Test (A2). Each register specified in the configuration contents defines the read-only and read/write bits. The test writes 0s and 1s to the test bits to ensure that the read-only bit values are not changed and that the read/write bits are changed.
		The test attempts to read the register configuration file (Miireg.txt) for the register definitions. If the file does not exist, the following table is used:
		`Offset  Read-Only Mask  Read/Write Mask`
		`0x00    0x0000          0x7180`
		`0x02    0xFFFF          0x0000`
		`0x03    0xFFFF          0x0000`
		`0x04    0x0000          0xFFFF`
		`0x05    0xEFFF          0x0000`
		`0x06    0x0001          0x0000`
		`0x07    0x0800          0xB7FF`
		`0x08    0xFFFF          0x0000`
		`0x09    0x0000          0xFF00`
		`0x0A    0x7C00          0x0000`
		`0x10    0x0000          0xFFBF`
		`0x11    0x7C00          0x0000`
		`0x19    0x7C00          0x0000`
		`0x1E    0x0000          0xFFFF`
		`0x1F    0x0000          0xFFFF`

C5	VPD	The VPD test first saves the contents of the vital product data (VPD) memory before performing the test. The test then writes 1 of the 5 test data patterns (0xFF, 0xAA, 0x55, increment data, or decrement data) into VPD memory. By default, an incremental data pattern is used. The test writes and reads back the data for the entire test range, and then restores the original contents of the VPD memory.
C6	ASF Hardware	**Reset Test.** This test sets the reset bit and polls for self-clearing bits. This test verifies the reset value of the registers. **Event Mapping Test.** This test sets the SMB_ATTN bit. By changing ASF_ATTN_ LOC bits, the test verifies the mapping bits in TX_CPU or RX_CPU event bits. Counter Test • Clears WG_TO, HB_TO, PA_TO, PL_TO, RT_TO bits (by setting the bits) and ensures that the bits clear. • Clears the timestamp counter. Writes a 1 to each of the PL, PA, HB, WG, RT counters. Sets the TSC_EN bit. • Polls each PA_TO bit and counts up to 50. Checks if the PL_TO bit is set at the end of the count to 50. Continues to count up to 200. Checks if all other TO bits are set and verifies if the timestamp counter is incremented.
C7	Expansion ROM	This test tests the ability to enable, disable, and access the expansion read-only memory (ROM) on the adapter.
C8	CPU Fetch	This test tests the PCU instruction fetch logic 100 times.
Group D: Driver Associated Tests		

Table 3: Diagnostic Tests (Cont.)

Test		*Description*
Number	***Name***	
D1	MAC Loopback	This test is an internal loopback data transmit/receive test. It initializes the medium access control (MAC) into an internal loopback mode and transmits 100 packets. The data should be routed back to the receive channel and received by the receive routine, which verifies the integrity of data. A 100-Mbit/s data rate is used for this test unless Gigabit Ethernet is enabled.
D2	PHY Loopback	This test is same as the MAC loopback test (D1), except that the data is routed back via a physical layer device (PHY). A 100-Mbit/s data rate is used for this test unless Gigabit Ethernet is enabled.
D5	MII Miscellaneous	This test tests the autopolling and PHY interrupt capabilities. These are functions of the PHY.
D6	MSI	This test tests the message signal interrupt (MSI) capability of the adapter. Refer to PCI Specification, version 2.3, for the MSI definition.

Diagnostic Test Messages

```
/* 0 */ "PASS",
/* 1 */ "Got 0x%08X @ 0x%08X. Expected 0x%08X",
/* 2 */ "Cannot perform task while chip is running",
/* 3 */ "Invalid NIC device",
/* 4 */ "Read-only bit %s got changed after writing zero
at offset 0x%X",
/* 5 */ "Read-only bit %s got changed after writing one
at offset 0x%X",
/* 6 */ "Read/Write bit %s did not get cleared after writing zero
at offset 0x%X",
/* 7 */ "Read/Write bit %s did not get set after writing one
at offset 0x%X",
/* 8 */ "BIST failed",
/* 9 */ "Could not generate interrupt",
/* 10 */ "Aborted by user",
/* 11 */ "TX DMA:Got 0x%08X @ 0x%08X. Expected 0x%08X",
/* 12 */ "Rx DMA:Got 0x%08X @ 0x%08X. Expected 0x%08X",
/* 13 */ "TX DMA failed",
/* 14 */ "Rx DMA failed",
/* 15 */ "Data error, got 0x%08X at 0x%08X, expected 0x%08X",
/* 16 */ "Second read error, got 0x%08X at 0x%08X, expected 0x%08X",
/* 17 */ "Failed writing EEPROM at 0x%04X",
/* 18 */ "Failed reading EEPROM at 0x%04X",
/* 19 */ "EEPROM data error, got 0x08X at 0x04X, expected 0x%08X",
/* 20 */ "Cannot open file %s",
/* 21 */ "Invalid CPU image file %s",
/* 22 */ "Invalid CPU image size %d",
/* 23 */ "Cannot allocate memory",
/* 24 */ "Cannot reset CPU",
/* 25 */ "Cannot release CPU",
/* 26 */ "CPU test failed",
/* 27 */ "Invalid Test Address Range\nValid NIC address is
0x%08X-0x%08X and exclude 0x%08X-0x%08X",
/* 28 */  "DMA:Got 0x%08X @ 0x%08X. Expected 0x%08X",
/* 29 */  "Unsupported PhyId %04X:%04X",
/* 30 */  "Too many registers specified in the file, max is %d",
/* 31 */ "Cannot write to VPD memory",
/* 32 */ "VPD data error, got %08X @ 0x04X, expected %08X",
/* 33 */ "No good link! Check Loopback plug",
/* 34 */ "Cannot TX Packet!",
/* 35 */ "Requested to TX %d. Only %d is transmitted",
/* 36 */"Expected %d packets. Only %d good packet(s) have been
received\n%d unknown packets have been received.\n%d bad packets
have been received.",
/* 37 */ "%c%d is an invalid Test",
/* 38 */ "EEPROM checksum error",
/* 39 */ "Error in reading WOL/PXE",
/* 40 */ "Error in writing WOL/PXE",
/* 41 */ "No external memory detected",
/* 42 */ "DMA buffer %04X is large, size must be less than %04X",
/* 43 */ "File size %d is too big, max is %d",
/* 44 */ "Invalid %s",
/* 45 */ "Failed writing 0x%x to 0x%x",
/* 46 */ "",
/* 47 */ "Ambiguous command",
/* 48 */ "Unknown command",
/* 49 */ "Invalid option",
/* 50 */ "Cannot perform task while chip is not running. (need driver)",
/* 51 */ "Cannot open register define file or content is bad",
/* 52 */ "ASF Reset bit did not self-clear",
/* 53 */ "ATTN_LOC %d cannot be mapped to %cX CPU event bit %d",
/* 54 */ "%s Register is not cleared to zero after reset",
/* 55 */ "Cannot start poll_ASF Timer",
/* 56 */ "poll_ASF bit did not get reset after acknowledged",
/* 57 */ "Timestamp Counter is not counting",
/* 58 */ "%s Timer is not working",
/* 59 */ "Cannot clear bit %s in %cx CPU event register",
/* 60 */ "Invalid "EEPROM_FILENAME" file size, expected %d but
only can read %d bytes",
/* 61 */ "Invalid magic value in %s, expected %08x but found %08x",
/* 62 */ "Invalid manufacture revision, expected %c but found %c",
/* 63 */ "Invalid Boot Code revision, expected %d.%d but found %d.%d",
/* 64 */ "Cannot write to EEPROM",
/* 65 */ "Cannot read from EEPROM",
/* 66 */ "Invalid Checksum",
/* 67 */ "Invalid Magic Value",
/* 68 */ "Invalid MAC address, expected %02X-%02X-%02X-%02X-%02X-%02X",
/* 69 */ "Slot error, expected an UUT to be found at location %02X:%02X:00",
/* 70 */ "Adjacent memory has been corrupted while testing block
0x%08x-0x%08x\nGot 0x%08x @ address 0x%08x. Expected 0x%08x",
/* 71 */ "The function is not Supported in this chip",
/* 72 */ "Packets received with CRC error",
/* 73 */ "MII error bits set: %04x",
/* 74 */ "CPU does not initialize MAC address register correctly",
/* 75 */ "Invalid firmware file format",
/* 76 */ "Resetting TX CPU Failed",
/* 77 */ "Resetting RX CPU Failed",
/* 78 */ "Invalid MAC address",
/* 79 */ "Mac address registers are not initialized correctly",
/* 80 */ "EEPROM Bootstrap checksum error",
```

Troubleshooting: Broadcom NetXtreme 57XX User Guide

NOTE: For additional information, go to *Broadcom Ethernet NIC Frequently Asked Questions* at http://www.broadcom.com/support/ethernet_nic/faq_drivers.php

HARDWARE DIAGNOSTICS

Loopback diagnostic tests are available for testing the adapter hardware. These tests provide access to the adapter internal/external diagnostics, where packet information is transmitted across the physical link. For Windows environments, see Running Diagnostic Tests).

BACS DIAGNOSTIC TESTS FAILURES

If any of the following tests fail while running the diagnostic tests from the Running Diagnostic Tests tab in BACS, this may indicate a hardware issue with the NIC or LOM that is installed in the system.

- Control Registers
- MII Registers
- EEPROM
- Internal Memory
- On-Chip CPU
- Interrupt
- Loopback - MAC
- Loopback - PHY
- Test LED

Below are troubleshooting steps that may help correct the failure.

1. Remove the failing device and reseat it in the slot, ensuring the card is firmly seated in the slot from front to back.
2. Rerun the test.
3. If the card still fails, replace it with a different card of the same model and run the test. If the test passes on the known good card, contact your hardware vendor for assistance on the failing device.
4. Power down the machine, remove AC power from the machine, and then reboot the system.
5. Remove and re-install the diagnostic software.
6. Contact your hardware vendor.

BACS Network Test Failures

Typically, the BACS Testing the Network failures are the result of a configuration problem on the network or with the IP addresses. Below are common steps when troubleshooting the network.

1. Verify that the cable is attached and you have proper link.
2. Verify that the drivers are loaded and enabled.
3. Replace the cable that is attached to the NIC/LOM.
4. Verify that the IP address is assigned correctly using the command "ipconfig" or by checking the OS IP assigning tool.
5. Verify that the IP address is correct for the network to which the adapter(s) is connected.

Troubleshooting Checklist

⚠

CAUTION! Before you open the case of your system, review Safety Precautions.

The following checklist provides recommended actions to take to resolve problems installing the Broadcom NetXtreme Gigabit Ethernet adapter or running it in your system.

- Inspect all cables and connections. Verify that the cable connections at the network adapter and the switch are attached properly. Verify that the cable length and rating comply with the requirements listed in Connecting the Network Cables.
- Check the adapter installation by reviewing Installing the Hardware. Verify that the adapter is properly seated in the slot. Check for specific hardware problems, such as obvious damage to board components or the PCI edge connector.
- Check the configuration settings and change them if they are in conflict with another device.
- Verify that your system is using the latest BIOS.
- Try inserting the adapter in another slot. If the new position works, the original slot in your system may be defective.
- Replace the failed adapter with one that is known to work properly. If the second adapter works in the slot where the first one failed, the original adapter is probably defective.
- Install the adapter in another functioning system and run the tests again. If the adapter passed the tests in the new system, the original system may be defective.
- Remove all other adapters from the system and run the tests again. If the adapter passes the tests, the other adapters may be causing contention.

Checking for Network Link and Activity

See Testing Network Connectivity or Viewing Adapter Information to check the state of the network link and activity as indicated by the port LEDs.

Checking if Current Drivers are Loaded

Windows

See Viewing Adapter Information to view useful information about the adapter, its link status, and network connectivity.

NetWare

To verify that the driver is loaded properly, type

```
LOAD B57.LAN FRAME_ETHERNET_II NAME=B57_1_EII
```

This command automatically verifies if the link is active. If the link is active, the command returns Link is up.

From the command line, type `config` then press ENTER. The following status information is displayed:

```
Broadcom NetXtreme Gigabit Ethernet Adapter
Version:
Hardware Setting:
Node Address:
Frame Type:
```

```
Board Name:
LAN Protocol: ARP (see note)
LAN Protocol: IP Addr: (see note)
```

NOTE: The LAN protocol status is displayed after an IP address is assigned to the adapter.

Linux

To verify that the TG3 Linux driver is loaded properly, run:

```
lsmod | grep tg3
```

If the driver is loaded, a line similar to the one below is displayed, where *size* is the size of the driver in bytes, and *n* is the number of adapters configured.

Table 1: Linux Driver

Module	*Size*	*Used by*
TG3	*size*	*n*

Running a Cable Length Test

In Windows environments, a cable length test can be run. See Analyzing Cables for information about running a cable length test.

Testing Network Connectivity

NOTE: When using forced link speeds, verify that both the adapter and the switch are forced to the same speed, or that both sides are configured for auto-negotiation.

Windows

Use the ping command to determine if the network connection is working.

NOTE: Network connectivity can also be tested using the Testing the Network feature in Broadcom Advanced Control Suite 2.

1. Click **Start**, and then click **Run**.
2. Type **cmd** in the **Open** box, and then click **OK**.
3. Type **ipconfig /all** to view the network connection to be tested.
4. Type **ping IP address**, and then press ENTER.

The ping statistics that are displayed indicate whether the network connection is working or not.

NetWare

Ping an IP host on the network to verify connection has been established:

From the command line, type **ping IP address**, and then press ENTER.

The ping statistics that are displayed indicate whether the network connection is working or not.

Linux

To verify that the Ethernet interface is up and running, run **ifconfig** to check the status of the Ethernet interface. It is possible to use **netstat -i** to check the statistics on the Ethernet interface. Go to Linux Driver Software for information on **ifconfig** and **netstat**.

Ping an IP host on the network to verify connection has been established:

From the command line, type **ping IP address**, and then press ENTER.

The ping statistics that are displayed indicate whether the network connection is working or not.

Software Problems and Solutions

How to Add a Third-Party OEM Network Adapter to a RIS Installation

Problem: An error is encountered when attempting to load the Broadcom device driver for a 32-bit version of Windows XP, or later operating system, using a Windows 2000 Remote Installation Server: *File b57w2k.sys caused an unexpected error (21) at line 3752 in d:\xpsp1\base\boot\setup\setup.c.*

Solution: A modification to the b57win32.inf file can be made to allow for the installation to complete successfully. This will be in conjunction with instructions from the Microsoft Knowledge Base Article 315279 that describe “How to Add Third-Party OEM Network Adapters to RIS Installations.”

Requirement: The Windows 2000 Server must be running Service Pack 3 or later.

1. Obtain the latest driver for your Broadcom adapter. The driver files included for the Broadcom 57xx adapter are b57win32.inf, b57win32.cat, and b57xp32.sys.
2. Create a copy of the b57win32.inf and b57xp32.sys files and save them in a separate folder called RIS. This allows you to distinguish the duplicate files from the originals.
3. For the b57win32.inf file located in the RIS folder, make the following change using a text editor such as Notepad:
    a. Locate **[Manufacturer]** within the file.
    b. Review the line below which reads: **%BRCM% = Broadcom, NTx86.5.1, NTamd64**.
    c. Modify that line to read: **%BRCM% = Broadcom.NTx86.5.1, NTamd64**. (The change replaces the comma and the space after “Broadcom” with a period.
    d. Save the file.
4. On the RIS server, copy the b57win32.inf and b57xp32.sys files from the RIS folder to the RemoteInstall\Setup\Language\Images\Dir_name\i386 folder. This allows Setup to use the driver during the text-mode portion of the installation.
    a. At the same level as the i386 folder on the RIS image, create a $oem$ folder. Use the recommended structure: \$oem$\$1\Drivers\Nic
    b. Copy the original b57win32.inf, b57xp32.sys, and b57win32.cat driver files to this folder.
    c. Make the following changes to the **.sif** file that is used for this image installation:

```
[Unattended]
OemPreinstall = yes
OemPnpDriversPath = \Drivers\Nic
```

5. Stop and then restart the Remote Installation service on the RIS server by typing the following from a command prompt:

```
net stop binlsvc
net start binlsvc
```

RIPREP Utility Problem

Problem: The following message is received when attempting to deploy a RIPREP image through Remote Installation Services (RIS): *"The operating system image you selected does not contain the necessary drivers for your network adapter. Try selecting a different operating system image. If the problem persists, contact your administrator. Setup cannot continue. Press any key to exit."*

Solution: This problem is not isolated to the Broadcom adapter. However, based on several inquiries, we are publishing the following instructions based on other customers successfully working around this issue:

1. Place the Broadcom driver files in the original image folder (the image folder created when risetup.exe was executed for the first time).
   Example: i:\RemoteInstall\Setup\English\Images\(Original Image)
2. Place the Broadcom driver files in the i386 subfolder under the original image folder.
   Example: i:\RemoteInstall\Setup\English\Images\(*Original Image*)\i386
3. Place the Broadcom driver files for the network adapter in the RIPREP Image folder.
   Example: i:\RemoteInstall\Setup\English\Images\(RIPREP Image)
4. Place the Broadcom adapter drivers in the i386 subfolder where the RIPREP Image is located.
   Example: i:\RemoteInstall\Setup\English\Images\(RIPREP Image)\i386

The Microsoft Knowledge base articles listed below were used as a reference for the following instructions:

http://support.microsoft.com/default.aspx?scid=kb;EN-US;254078

http://support.microsoft.com/default.aspx?scid=kb;EN-US;246184

5. Create the following path and place all Broadcom driver files in ..\(*RIPREP Image*)\$oem$\$1\Drivers.
6. Edit the riprep.sif file located in ..\(*RIPREP Image*)\i386\Template to include the following information under the [Unattend] section:

```
OemPreinstall = yes
OemPnPDriversPath = "Drivers
DriverSigningPolicy = Ignore
```

7. Create the following path and place all Broadcom driver files in ..\(*Original Image*)\$oem$\$1\Drivers.
8. Edit the ristndrd.sif file located in ..\(*Original Image*)\i386\templates to include the following information under the [Unattend] section:

```
OemPreinstall = yes
OemPnPDriversPath = "Drivers
DriverSigningPolicy = Ignore
```

9. Restart the Remote Installation service. This can be performed from a command line with the following commands:

```
net stop binlsvc
net start binlsvc
```

Using the System Preparation Tool

Problem: I want to be sure that my Broadcom NetXtreme adapter works properly if I use the System Preparation utility (Sysprep.exe) to install an existing configuration on my system.

Solution: On the Sysprep.inf file, modify the [Unattend] header as shown below:

```
[Unattend]
OemPnPDriversPath=Drivers\Net
OemPreinstall = Yes
```

The driver files for the Broadcom NetXtreme adapter must reside in this folder, which is located on the system drive (where the operating system resides). If other drivers are to be loaded, then **Drivers\Net** can be appended to the paths listed and separated by a semicolon:

Example:

```
OemPnpDriversPath=Drivers\Video;Drivers\Net
```

The Sysprep utility must run with the **–pnp** switch, which enables the system to rescan for new devices that can be added during the mini-setup.

A Sample Sysprep.inf file for Windows XP is shown below.

```
------------------------------------------------------------------------
;SetupMgrTag
[Unattended]
OemSkipEula=Yes
OemPreinstall=Yes
TargetPath=\Windows
UnattendedInstall=Yes
OemPnpDriversPath=Drivers\Net
[GuiUnattended]
AdminPassword="password"
EncryptedAdminPassword=NO
AutoLogon=Yes
AutoLogonCount=99
OEMSkipRegional=1
OEMDuplicatorstring="XP System"
TimeZone=4
OemSkipWelcome=1
[UserData]
FullName="User"
OrgName="Organization"
ComputerName=*
[SetupMgr]
DistFolder=C:\sysprep\i386
DistShare=whistlerdist
[Identification]
JoinDomain=workgroup
[Networking]
InstallDefaultComponents=Yes
------------------------------------------------------------------------
```

LINUX AND ASFIPMON

Problem: I brought down the interface and now I cannot bring it back up. When I try, the following message appears, ‘SIOCSIFFLAGS: Resource temporarily unavailable.’
Solution: When ASFIPMon is running, it does a quick access to flash ROM every 30 seconds or so. If the interface is brought down while this is happening, you cannot bring the interface back up in the usual way. To bring up the interface, unload and then reload the driver module.

BROADCOM BOOT AGENT

Problem: Unable to obtain network settings through DHCP using PXE.
Solution: For proper operation make sure that the Spanning Tree Protocol (STP) is disabled or that portfast mode (for Cisco) is enabled on the port to which the PXE client is connected. For instance, set spantree portfast 4/12 enable.

BROADCOM ADVANCED SERVER PROGRAM (BASP)

Problem: After physically removing a NIC that was part of a team and then rebooting, the team did not perform as expected.
Solution: To physically remove a teamed NIC from a system, you must first delete the NIC from the team. Not doing this before shutting down could result in breaking the team on a subsequent reboot, which may result in unexpected team behavior.

Problem: The 802.3ad team member links disconnect and reconnect continuously (applies to all operating systems).
Solution: This is a third-party issue. It is seen only when configuring an 802.3ad team with more than 2 members on the system and connecting to an HP2524 switch, with LACP enabled as passive or active. The HP switch shows an LACP channel being brought up successfully with only 2 team members. All other team member links disconnect and reconnect. This does not occur with a Cisco Catalyst 6500.

Problem: A Generic Trunking (GEC/FEC) 802.3ad-Draft Static type of team may lose some network connectivity if the driver to a team member is disabled.
Solution: If a team member supports underlying management software (ASF/IPMI/UMP) or Wake-On-LAN, the link may be maintained on the switch for the adapter despite its driver being disabled. This may result in the switch continuing to pass traffic to the attached port rather than route the traffic to an active team member port. Disconnecting the disabled adapter from the switch will allow traffic to resume to the other active team members.

Problem: The teaming changes I made when I modified my team using INETCFG did not take effect.
Solution: When you modify a team using INETCFG, you may need to reboot after reinitialization for the changes to the team to take effect.

MISCELLANEOUS

Problem: Although installled, the Broadcom Advanced Control Suite (BACS) application does not start.
Solution: .NET Framework 2.0 is required for BACS to operate. Install .NET Framework 2.0.

Problem: When the bus on the system is operating in PCI mode, the Broadcom NetXtreme Gigabit Ethernet adapter performs at PCI mode if it is added after the system has booted.
Solution: When the system is booted up without any adapter, the bus operates at the lowest mode, which is PCI mode. Reboot the system after the adapter has been added.

Problem: The Broadcom NetXtreme Gigabit Ethernet adapter may not perform at optimal level on some systems if it is added after the system has booted.
Solution: The system BIOS in some systems does not set the cache line size and the latency timer if the adapter is added after the system has booted. Reboot the system after the adapter has been added.

Problem: Large Send Offload (LSO) and Checksum Offload are not working on my team.
Solution: If one of the adapters on a team does not support LSO, LSO does not function for the team. Remove the adapter that does not support LSO from the team, or replace it with one that does. The same applies to Checksum Offload.

Problem: When using the TG3 driver and Red Hat 4 (with any release prior to release 6), after setting the speed and duplex with ethtool, autonegotiation is disabled and cannot be restored.
Solution: Unload or reload the TG3 driver, or upgrade to the latest version of ethtool.

Problem: A DCOM error message (event ID 10016) appears in the System Even Log during the installation of the Broadcom adapter drivers.
Solution: This is a Microsoft issue. For more information, see Microsoft knowledge base KB913119 at http://support.microsoft.com/kb/913119.